RGPD

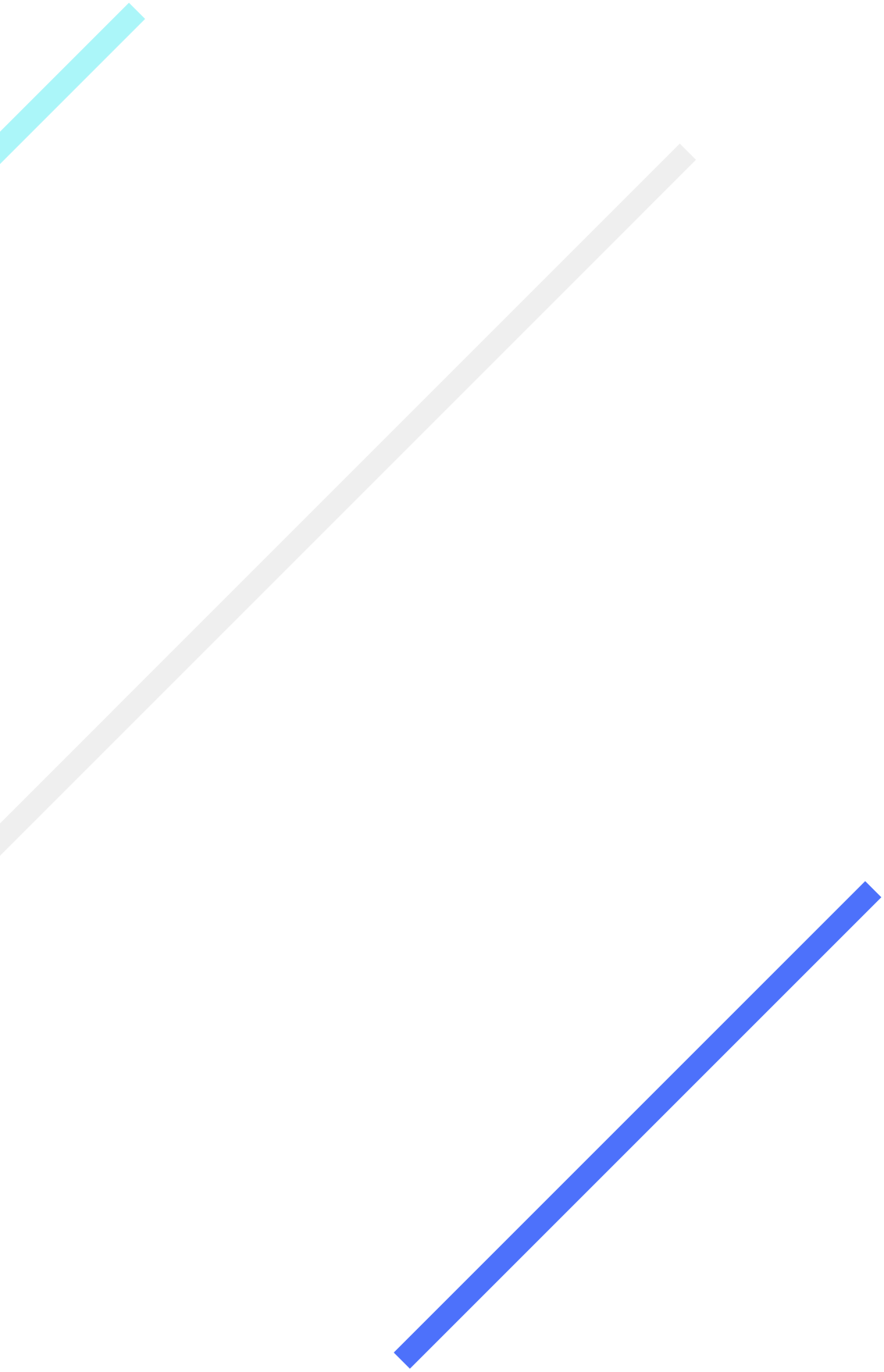
Guide actualisant le Pack de conformité Assurance

CTIP
CENTRE TECHNIQUE DES INSTITUTIONS DE PRÉVOYANCE

Fédération Française de l'Assurance

PLANETE CSCA

MUTUALITÉ FRANÇAISE



Guide actualisant les principes inscrits dans le pack de conformité assurance de la CNIL

rédigé en association avec la CNIL

PÉRIMÈTRE

Ce document s'adresse aux responsables du traitement ayant la qualité « d'organisme d'assurance ». Cette notion regroupe les entreprises d'assurance (sociétés anonymes d'assurance et sociétés d'assurance mutuelles relevant du Code des assurances, mutuelles relevant du Code de la mutualité et institutions de prévoyance relevant du Code de la sécurité sociale), de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance et/ou de réassurance.

Lexique

En assurance, la notion de partie au contrat tel que cela est prévu par le RGPD doit s'entendre de toute personne partie, intéressée ou intervenant au contrat. Outre l'assureur, il peut s'agir des personnes suivantes :

Adhérent

Personne qui adhère soit à un contrat individuel ou règlement, soit à un contrat collectif facultatif ou obligatoire souscrit par une personne morale au profit des membres.

Agent général[1]

Professionnel indépendant exerçant l'activité d'intermédiaire pour le compte d'une compagnie d'assurance dont il a reçu un mandat.

AGIRA

Association pour la Gestion des Informations sur le Risque en Assurance. L'AGIRA a été créée par la Fédération Française de l'Assurance (FFA) et regroupe les sociétés d'assurance exerçant sur le marché français et les organisations professionnelles intervenant dans le secteur. Organisme professionnel de l'assurance, l'AGIRA met en œuvre des dispositifs soit par les pouvoirs publics, soit par la profession, à destination d'une part, du public et des assurés et d'autre part, des assureurs et de leurs partenaires (ex : recherche des contrats d'assurance-vie / dépendance / obsèques, Fichier des véhicules assurés « FVA », etc).

ALFA

Agence pour la Lutte contre la Fraude à l'Assurance - association dont l'objet est de promouvoir la lutte contre la fraude dans le secteur de l'assurance. L'ALFA compte plus de 320 adhérents, pour la plupart membres de la FFA. Les autres organismes d'assurance affiliés à ALFA sont des mutuelles régies par le livret II du Code de la mutualité, des institutions de prévoyance, des réassureurs ou encore des entreprises en libre prestation de service.

Assuré

Personne qui bénéficie des garanties du contrat d'assurance.

À titre d'exemples :

- En matière d'assurance automobile, l'assuré est le propriétaire du véhicule. L'assuré est aussi « toute personne » qui, avec l'autorisation dudit propriétaire, possède la garde du véhicule ou le conduit.
- En matière d'assurance habitation, l'assuré est le souscripteur mais aussi son conjoint, ses enfants mineurs et/ou majeurs qui vivent sous le même toit à l'adresse figurant sur le contrat d'assurance. Certains assureurs admettent aussi que toute autre personne résidant en permanence sous le même toit à l'adresse indiquée sur les conditions particulières, puisse également être considérée comme assuré.
- En matière d'assurance de personnes, l'assuré est généralement le souscripteur du contrat sur lequel repose le risque (décès, maladie, invalidité, incapacité, dépendance, retraite, accident) soit l'adhérent ou le membre participant.

Ayant droit

Personne qui détient un droit en raison de sa situation juridique, fiscale, financière ou d'un lien familial avec le bénéficiaire direct de ce droit.

Bénéficiaire

Personne au profit de laquelle une assurance a été contractée. Elle peut être nommément désignée aux conditions particulières du contrat ou bien être désignée de manière générale dans les conditions générales. Le bénéficiaire recevra l'indemnité due par l'assureur en cas de réalisation du risque assuré.

Co-conception de produits d'assurance

Le processus de conception et de mise à jour des produits d'assurance est visé par l'article 25 de la directive distribution d'assurance et complété par le règlement délégué du 21/09/2017 sur la gouvernance et la surveillance des produits (GSP)[2]. Certains intermédiaires peuvent être considérés comme

[1] Article R 511-2-I-2° du Code des assurances : les agents généraux d'assurance, personnes physiques ou personnes morales, titulaires d'un mandat ou chargées à titre provisoire pour une durée de deux ans au plus non renouvelables des fonctions d'agent général d'assurance. Ces personnes exercent la distribution selon les modalités mentionnées au a) du II de l'article L. 521-2.

[2] Notamment les articles 3.1 et 3.4 du Règlement délégué : «les intermédiaires d'assurance sont considérés comme des concepteurs lorsqu'une analyse globale de leur activité montre qu'ils ont un rôle décisionnel dans l'élaboration et la mise au point d'un produit d'assurance destiné au marché » [...] « Un intermédiaire d'assurance et une entreprise d'assurance qui sont tous deux concepteurs au sens de l'article 2 du présent règlement délégué signent un accord écrit qui précise comment ils collaborent pour respecter les exigences applicables aux concepteurs visées à l'article 25, paragraphe 1, de la directive (UE) 2016/97, les procédures au moyen desquelles ils conviennent de la définition du marché cible et leurs rôles respectifs dans le processus d'approbation de produit ».

co-concepteurs du produit, s'ils agissent en tant que tels. Sont systématiquement considérés comme des concepteurs les assureurs en tant que porteurs des risques. Les engagements qu'ils portent vis-à-vis des assurés motivent ce principe.

Courtier d'assurance[3]

Intermédiaire d'assurance – personnes physiques et sociétés immatriculées au registre du commerce pour l'activité de courtage d'assurance - dont la profession est réglementée par le Code des assurances. Il doit satisfaire au devoir de conseil et à l'obligation d'information auxquels la législation soumet toute personne habilitée à proposer et à vendre des contrats d'assurance.

Co-assureur

La coassurance est l'opération consistant à associer plusieurs assureurs dans la couverture d'un ou plusieurs risques d'un même assuré. Elle peut porter sur le même risque, qui se trouve alors assuré par plusieurs assureurs qui partagent le même risque selon une répartition convenue. Elle peut également porter sur des risques différents, chaque assureur ne couvrant qu'un seul ou plusieurs risques sans partage avec les autres assureurs (par exemple, un assureur procure les garanties dommages aux biens tandis qu'un autre procure les garanties d'assistance).

Délégataire de gestion pour les compagnies d'assurance

Moyen d'externaliser tout ou partie de leurs activités en confiant par mandat certains processus de souscription et/ou gestion d'un contrat. Ces activités sont alors confiées à un organisme, le délégataire, qui est en chargé de répondre aux besoins des assurés de la compagnie en s'appuyant sur ses propres ressources humaines, financières, etc.

Expert

Les experts sont des spécialistes dans leur domaine permettant de qualifier un risque, un dommage, de l'évaluer et de le chiffrer en toute indépendance. Ils peuvent faire partie d'une profession réglementée comme les experts médicaux ou experts automobiles, ou non réglementée tels que les experts intervenant pour le risque habitation.

Intermédiaire en assurance et réassurance

Toute personne physique ou morale autre qu'une entreprise d'assurance ou de réassurance qui, contre rémunération, accède à l'activité de distribution d'assurances ou de réassurances ou l'exerce. La distribution d'assurances ou de réassurances est l'activité qui consiste à fournir des recommandations sur des contrats d'assurance ou de réassurance, à présenter, à proposer, à aider à conclure ou concevoir des contrats ou à réaliser d'autres travaux préparatoires à leur conclusion, ou à contribuer à leur gestion et à leur exécution, notamment en cas de sinistre.

Mandataire d'assurance[4]

Personne physique non salariée ou personne morale directement mandatée par une entreprise d'assurance. Il intervient pour la compagnie avec ou sans exclusivité.

Mandataire d'intermédiaires en assurance[5]

Professionnel agissant dans le cadre d'un mandat écrit délivré par un courtier d'assurance, un agent général ou un mandataire d'assurance, et dont l'activité est la présentation, la proposition ou l'aide à la conclusion d'une opération d'assurance. Sous réserve qu'il bénéficie d'un contrat d'encaissement, le MIA peut également encaisser les primes d'assurance.

Organisme d'assurance

Cette notion regroupe les entreprises d'assurance (sociétés anonymes d'assurance et sociétés d'assurance mutuelles relavant du Code des assurances, mutuelles relevant du Code de la mutualité et institutions de prévoyance relavant du Code de la sécurité sociale), de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance et/ou de réassurance (agents généraux d'assurance, mandataires et courtiers d'assurance).

[3] Article R 511-2-I-1° du Code des assurances : les courtiers d'assurance ou de réassurance, personnes physiques et sociétés immatriculées au registre du commerce pour l'activité de courtage d'assurance. Ces personnes exercent la distribution selon les modalités mentionnées aux b) ou c) du II de l'article L. 521-2.

[4] Article R 511-2, I, 3 du Code des assurances : personnes physiques non salariées et personnes morales autres que les agents généraux d'assurance, mandatées à cet effet par une entreprise d'assurance. Ces personnes exercent leur activité selon les modalités mentionnées au a) ou b) du II de l'article L. 521-2.

[5] Article R 511-2, I, 4° du Code des assurances : personnes physiques non salariées et personnes morales mandatées par une personne physique ou une personne morale mentionnée aux 1°, 2°, 3° ou 6° du présent article.

Réassurance

La réassurance est l'opération par laquelle un assureur s'assure lui-même auprès d'une autre société (le réassureur) pour tout ou partie des risques qu'il a pris en charge. Elle peut porter sur un ou plusieurs contrats d'assurance sous-jacents.

SINTIA

Le Groupement d'Intérêt Économique « SINTIA » pilote, pour le compte de la FFA, des projets de dématérialisation en assurance santé et collective, la création de sites internet, d'outils et de normes permettant d'automatiser les flux d'informations entre les assureurs santé ou collectifs et d'autres acteurs, par exemple les professionnels et établissements de santé, les caisses d'assurance maladie obligatoire, les assureurs, les délégataires de gestion, etc. Ses membres sont exclusivement des adhérents de la FFA, qui en est l'administrateur unique.

Souscripteur

Personne physique ou morale qui conclut le contrat d'assurance. Il peut être différent de l'assuré ou du bénéficiaire.

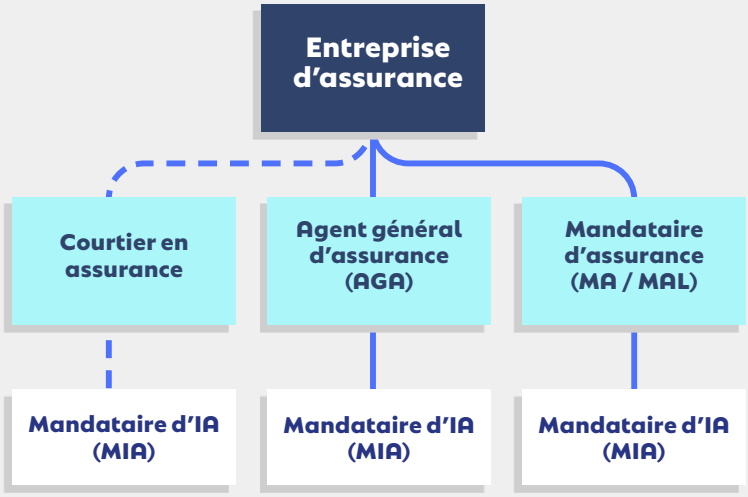
Tiers victime / Tiers réclamant

Le tiers est généralement défini comme une personne n'ayant pas la qualité d'assuré ou de bénéficiaire. Cette notion est utilisée principalement dans le cadre des contrats d'assurance contenant des garanties de responsabilité civile.
L'objet du contrat d'assurance de responsabilité est de garantir les conséquences pécuniaires de la responsabilité pouvant incomber à l'assuré en cas de dommages causés aux tiers. En droit français, le tiers victime, également appelé tiers réclamant, dispose d'une action directe contre l'assureur sur le fondement du contrat d'assurance.

Autres parties intéressées ou intervenant au contrat

Il s'agit notamment des organismes de tiers payant, avocats, médecins, professionnels de santé et réseaux de soins, experts, enquêteurs, officiers ministériels tels que les huissiers et les notaires, témoins, curateurs, tuteurs, cautions, autres entités du groupe auquel appartient l'assureur ou le réassureur concerné, autres entreprises d'assurance concernées par le contrat tels que l'assureur de protection juridique du tiers victime, organismes de Sécurité Sociale, organismes professionnels, délégataires de souscription et/ou de gestion, prestataires, etc.

Les principaux acteurs en assurance



1

Qualification des acteurs du secteur de l'assurance au regard du RGPD

Rappel des différentes qualifications prévues par le RGPD

Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités et les moyens du traitement**:

- La détermination de la « finalité » du traitement est réservée au(x) « responsable(s) du traitement(s) ». Toute personne qui prend cette décision est donc un responsable du traitement.

- En revanche, la détermination des « moyens » du traitement peut être déléguée par le responsable du traitement, pour autant qu'elle concerne des questions techniques ou d'organisation. Ainsi, il est tout à fait possible que les moyens techniques et d'organisation (ex: matériel informatique, logiciel utilisé) soient déterminés exclusivement par le sous-traitant des données, sous la responsabilité du responsable de traitement[6]. **La détermination des moyens emporte la qualification de responsable de traitement uniquement lorsqu'elle concerne les éléments essentiels des moyens,** par exemple, sans que cette liste puisse être considérée comme exhaustive: la détermination des données à traiter ou des personnes pouvant les utiliser, les personnes concernées, les destinataires, les durées de conservation des données.

- L'accès aux données n'est pas un critère de qualification (le responsable n'a pas forcément accès aux données).

[6] Même si les décisions relatives aux moyens « non-essentiels » peuvent être laissées au sous-traitant, le responsable du traitement doit néanmoins stipuler certains éléments dans l'accord avec le sous-traitant, tels que - en ce qui concerne l'exigence de sécurité, par exemple une instruction de prendre toutes les mesures requises en vertu de l'article 32 du RGPD. Le contrat doit également stipuler que le sous-traitant doit aider le responsable du traitement à assurer le respect, par exemple, de l'article 32. En tout état de cause, le responsable du traitement reste responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour garantir et pouvoir démontrer que le traitement est effectué conformément au règlement (article 24 du RGPD).

Lorsque deux responsables du traitement ou plus **déterminent conjointement les finalités[7] et les moyens du traitement, ils sont les responsables conjoints du traitement**, pour la portion du traitement pour laquelle elle détermine conjointement les finalités. Si une entité décide seule les finalités et les moyens des opérations de traitement qui précèdent ou suivent la chaîne de traitement, cette entité doit être considérée comme l'unique responsable de traitement pour ces opérations.

Le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre **organisme distinct du responsable de traitement et agissant pour le compte du responsable du traitement.**

Attention : La qualification au sens du RGPD du rôle des parties dans le cadre d'un traitement de données à caractère personnel se fait indépendamment des éventuelles autres qualifications prévues par d'autres réglementations. Ainsi, par exemple, en droit des assurances, la notion de sous-traitance est également utilisée par la réglementation Solvabilité 2 qui la définit comme : *un accord, quelle que soit sa forme, conclu entre une entreprise d'assurance ou de réassurance et un prestataire de services, soumis ou non à un contrôle, en vertu duquel ce prestataire de services exécute, soit directement, soit en recourant lui-même à la sous-traitance, une procédure, un service ou une activité, qui serait autrement exécuté par l'entreprise d'assurance ou de réassurance elle-même.*

Critères de qualification[8]

Pour apprécier qui détermine les finalités et moyens du traitement, doivent être pris en compte les critères suivants :

- Le degré de précision des instructions préalables données par le responsable du traitement, qui détermine **la marge de manœuvre laissée au sous-traitant** ;
- Le degré de **contrôle et de surveillance** exercé par le responsable du traitement sur les données personnelles ;
- La **visibilité/l'image donnée par le responsable du traitement à la personne concernée**, et les attentes que cette visibilité suscite chez les personnes concernées.

Les questions suivantes doivent donc être posées pour déterminer qui est responsable du traitement :

- Pourquoi ce traitement a-t-il lieu ? **Qui a décidé les finalités du traitement ?**
- **Qui a décidé les éléments essentiels des traitements :** quelles données personnelles, quelles personnes concernées, quels destinataires, quelles durées de détention, etc ?
- **Comment sont décidés les moyens des traitements à mettre en œuvre** et qui décide d'avoir recours à des prestataires ?
- **Quel est le niveau de détail des instructions données à celui qui réalise les traitements ?** Sur quels domaines portent ces instructions ?
- **Quelle est l'autonomie et l'indépendance de celui qui réalise le traitement ?**
- Quel est le niveau de surveillance sur l'exécution du traitement ?
- Est-il possible d'auditer les opérations de traitement réalisées ?
- Qui détermine et qui est responsable de l'application des mesures de sécurité ?
- **Vis-à-vis des personnes concernées, quel organisme est visible/qui a une relation directe avec les personnes concernées ?**
- Qui définit l'information à fournir aux personnes concernées et qui se charge de la délivrer ?
- **Qui se charge de répondre aux demandes d'exercice des droits des personnes concernées ?**

[7] Ce sera le cas lorsque les parties traitent les données pour une finalité commune ou pour des finalités qui sont très liées ou complémentaires, sans que cela implique une responsabilité égale de tous les acteurs dans le traitement de données. En particulier, si une partie développe des moyens de traitement, qu'elle met à disposition d'autres entités, les entités qui décident d'utiliser ces moyens participent à la détermination des moyens du traitement. C'est le cas notamment avec des plateformes, outils standardisés ou autres infrastructures qui permettent aux parties de traiter des données, et qui ont été paramétrés d'une certaine manière par une partie afin d'être utilisés par d'autres parties, qui peuvent également décider du paramétrage. L'utilisation d'un système technique existant n'exclut pas la responsabilité conjointe dès lors que les utilisateurs du système peuvent décider du traitement de données à mettre en œuvre dans ce contexte. A l'inverse, le fait d'utiliser un système de traitement ou une infrastructure commune ne résultera pas systématiquement en une responsabilité conjointe, si les traitements mis en œuvre par les uns et les autres sont séparables et peuvent être effectués sans l'intervention des autres.

[8] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 – 7 novembre 2019.

Facteurs militant en faveur de la qualification en tant que responsable de traitement

- L'obtention d'un avantage ou l'existence d'un intérêt dans le traitement (autre que le simple paiement de services reçus d'un autre responsable du traitement);

- La prise de décisions à l'égard des personnes concernées dans le cadre ou à la suite du traitement (par exemple, les personnes concernées sont des employés de l'organisme);

- Les activités de traitement peuvent être considérées comme naturellement attachées au rôle ou aux activités de l'organisme (par exemple en raison de rôles traditionnels ou de compétences professionnelles), ce qui implique des responsabilités du point de vue de la protection des données;

- Le traitement concerne la relation de l'organisme avec les personnes concernées en tant qu'employés, clients, membres etc;

- Une autonomie totale pour décider de la manière dont les données à caractère personnel sont traitées;

- Le fait d'avoir confié le traitement de données à caractère personnel à une organisation externe chargée de traiter les données à caractère personnel au nom de l'organisme.

Un sous-traitant peut quant à lui décider des moyens « non-essentiels » suivants (non-exhaustif):
• système d'information ou autre moyen technique utilisé pour le traitement;
• méthode de stockage des données;
• niveau de sécurité appliqué aux données;
• détail des mesures de sécurité basées sur les objectifs généraux de sécurité fixés par le responsable de traitement;
• moyens utilisés pour transférer les données à une autre organisation;
• moyens utilisés pour permettre au responsable de traitement de mettre en œuvre les droits des personnes sur leurs données.

Facteurs militant en faveur de la qualification en tant que sous-traitant

- traitement des données à caractère personnel pour les besoins d'une autre partie et conformément à ses instructions documentées;

- absence d'objectif propre pour le traitement;

- une autre partie surveille les activités de traitement de l'organisme afin de s'assurer que ce dernier respecte les instructions et les termes du contrat;

- l'organisme ne poursuit pas sa propre finalité dans le cadre du traitement, autre que son propre intérêt commercial pour la fourniture de services;

- l'organisme a été engagé pour effectuer des activités de traitement par une personne qui, elle-même, a été engagée pour traiter des données au nom d'une autre partie et pour le compte de cette partie (sous-traitance ultérieure).

Exemples de qualifications

Les tableaux ci-après identifient des hypothèses de qualification juridique des acteurs du traitement en fonction de la nature de la relation contractuelle liant ces derniers et à partir des critères présentés précédemment. Les qualifications juridiques figurant dans le présent document sont renseignées à titre indicatif, de sorte que les acteurs du traitement demeurent libres d'apprécier les conditions particulières du traitement et de retenir, le cas échéant, une conclusion différente de celle établie dans ledit tableau.

Les exemples de qualifications suivantes s'entendent au regard du RGPD et n'interdisent pas d'autres qualifications notamment au regard d'autres législations.

Courtier et Preneur d'assurance

Relation Contractuelle	Contrat de courtage
Traitement nécessitant des données personnelles	✎ Opérations de prospection ✎ Devoir de conseil ✎ Etude du risque et/ou des conditions de couverture ✎ Placement du contrat ✎ Gestion et suivi de la clientèle ✎ Assistance en cas de sinistre (déclaration des sinistres, conseil pour l'acceptation des offres d'indemnité) ✎ Gestion des polices d'assurance (gestion administrative, gestion technique) ✎ Lutte contre le blanchiment des capitaux et le financement du terrorisme ✎ Lutte contre la fraude ✎ Traitement des réclamations portant sur l'activité spécifique du courtier
Détermination des finalités	**Par le courtier**
Détermination des moyens essentiels	**Par le courtier**
Détermination des moyens non-essentiels[9]	**Par le courtier**
Degré de contrôle	**Responsabilité du courtier**
Transparence et perception des personnes concernées	**Marque du courtier apparente**

Conclusion
Le courtier est le responsable du traitement

[9] Choix du système IT ou des outils techniques utilisés pour le traitement des données, détail des mesures de sécurité sur la base d'objectifs imposés par une autre partie…

Assureur et Preneur d'assurance (personne privée ou publique) Quel que soit le canal de distribution et sans délégation de gestion

Relation Contractuelle	Contrat d'assurance, ou d'assistance[10]
Traitement nécessitant des données personnelles	✎ Ensemble des traitements répondant aux finalités passation, gestion et exécution des contrats d'assurance (voir infra) ✎ Ensemble des traitements répondant aux finalités lutte contre la fraude/ LCB-FT ✎ Ensemble des traitements répondant aux finalités de prospection commerciale (voir infra).
Détermination des finalités	**Par l'assureur**
Détermination des moyens essentiels	**Par l'assureur**
Détermination des moyens non-essentiels	**Par l'assureur**
Degré de contrôle	**Responsabilité de l'assureur**
Transparence et perception des personnes concernées	**Par l'assureur**

Conclusion
L'assureur est le responsable du traitement
(Le statut de personne publique ou l'existence d'un appel d'offres n'a pas d'impact sur la qualification RGPD)

Dans l'hypothèse d'un contrat d'assurance co-conçu par l'assureur et le courtier, une coresponsabilité de ces deux acteurs pourrait être retenue (par exemple, lorsque le courtier définit – dans le cadre de cette co-conception – les finalités et les moyens essentiels du traitement). La co-conception d'un produit d'assurance peut être un indice d'une situation de co-responsabilité si au stade de la mise en œuvre des traitements, on constate que les critères précédemment exposés sont réunis.

Pour mémoire, le courtier est considéré comme co-concepteur lorsqu'il décide de manière autonome des caractéristiques essentielles d'un produit d'assurance et de ses principaux éléments y compris la couverture, les coûts, les risques, le marché cible ou les droits d'indemnisation ou de garantie et qu'il trouve un porteur de risque qui accepte ces conditions[11].

[10] Au sens de l'article R321-1 du Code des assurances
[11] Règlement délégué (UE) 2017/2358 de la Commission du 21 septembre 2017 complétant la directive (UE) 2016/97 du Parlement européen et du Conseil en ce qui concerne les exigences de surveillance et de gouvernance des produits applicables aux entreprises d'assurance et aux distributeurs de produits d'assurance

Assureur et Délégataire
Délégation de gestion avec autonomie limitée du délégataire (notamment auprès d'un courtier)[12]

Relation Contractuelle	Convention de délégation
Traitement nécessitant des données personnelles	✎ Gestion de la clientèle : souscription, gestion des adhésions, gestion des contrats, gestion des sinistres, envoi des termes, encaissement des primes etc ✎ Gestion des réclamations portant sur une activité déléguée ✎ Lutte contre la fraude ✎ LCB-FT
Détermination des finalités	**Par l'assureur** *Exemple : L'assureur détermine et contrôle des étapes de conclusion et d'exécution du contrat*
Détermination des moyens essentiels	**Par l'assureur** *Exemple : Détermination des données qui doivent être recueillies pour la conclusion et l'exécution du contrat par l'assureur. L'expertise du délégataire n'est pas prépondérante dans le traitement réalisé.*
Détermination des moyens non-essentiels	**Par l'assureur** *Exemple : Le délégataire se conforme aux processus définis par le seul assureur et utilise les outils informatiques mis à disposition par ce dernier (par exemple : un extranet)*
Degré de contrôle	**Par l'assureur** *Exemple : Reporting détaillé et audit transmis par le délégataire à l'assureur*
Transparence et perception des personnes concernées	**La marque de l'assureur est prépondérante** *Exemple : Produit standard à la marque de l'assureur mis à disposition de l'ensemble des apporteurs*

Conclusion
L'assureur est le responsable du traitement
Le délégataire est le sous-traitant

Par ailleurs, ce tableau ne vise que les traitements correspondant aux actes délégués dans le cadre d'une convention de gestion. Dans le cas où le délégataire est par ailleurs courtier en assurances, il est amené à réaliser des actes distincts à finalité de courtage, pour son propre compte. Il convient pour ceux-ci de consulter le tableau « Courtier et preneur d'assurance » ci-avant.

[12] Attention : l'étendue des actes délégués peut varier d'un contrat à l'autre. Il conviendra donc de retenir une analyse traitement par traitement afin de déterminer les portions du traitement effectuées sous la responsabilité conjointe de l'assureur et du délégataire, et les distinguer de celles qui sont effectuées sous l'unique responsabilité de l'une des parties.

Assureur et Délégataire
Délégation de gestion avec autonomie importante du délégataire (notamment auprès d'un courtier)[13]

Relation Contractuelle	Convention de délégation
Traitement nécessitant des données personnelles	✎ Gestion de la clientèle : souscription, gestion des adhésions, gestion des contrats, gestion des sinistres, envoi des termes, encaissement des primes, etc ✎ Gestion des réclamations portant sur une activité déléguée ✎ Lutte contre la fraude ✎ LCB-FT
Détermination des finalités	**Par l'assureur et le délégataire** *Exemple : Co-conception des contrats d'assurance (produits conçus par le courtier, le risque étant porté par un ou plusieurs assureurs).*
Détermination des moyens essentiels	**Par l'assureur et/ou le courtier délégataire** *Exemple : Détermination des processus de traitement pour la conclusion et l'exécution du contrat par le délégataire*
Détermination des moyens non-essentiels	**Par l'assureur et/ou le courtier délégataire** *Exemple : Détermination des systèmes d'informations par le délégataire*
Degré de contrôle	**Par l'assureur** *Exemple : Reporting détaillé et audit transmis par le délégataire à l'assureur*
Transparence et perception des personnes concernées	**La marque du délégataire est prépondérante** (l'identité de l'assureur doit toujours être indiquée)

Conclusion
L'assureur et le délégataire sont responsables conjoints du traitement

Par ailleurs, ce tableau ne vise que les traitements correspondant aux actes délégués dans le cadre d'une convention de gestion. Dans le cas où le délégataire est par ailleurs courtier en assurances, il est amené à réaliser des actes distincts à finalité de courtage, pour son propre compte. Il convient pour ceux-ci de consulter le tableau « Courtier et preneur d'assurance » ci-avant.

[13] Attention : l'étendue des actes délégués peut varier d'un contrat à l'autre. Il conviendra donc de retenir une analyse traitement par traitement.

Agent général et Assureur

Relation Contractuelle	**Mandat donné par l'assureur à l'agent général**	**Hors-Mandat donné par l'assureur à l'agent général**
Traitement nécessitant des données personnelles	✎ Ensemble des traitements répondant aux finalités passation, gestion et exécution des contrats d'assurance dans le cadre du mandat ✎ Lutte contre la fraude / LCB-FT ✎ Ensemble des traitements répondant aux finalités de prospection commerciale dans le cadre du mandat y compris par l'utilisation du fichier de portefeuille de clients qui lui est confié par l'assureur	✎ Opérations de prospection à l'initiative de l'agent et selon les modalités qu'il définit ✎ Services dérivés aux clients non prévus par le mandat pour son activité propre ✎ Courtage accessoire ✎ (voir supra)
Détermination des finalités	**Par l'assureur**	**Par l'agent**
Détermination des moyens essentiels	**Par l'assureur**	**Par l'agent**
Détermination des moyens non-essentiels	**Par l'assureur**	**Par l'agent**
Degré de contrôle	**Par l'assureur** Instructions précises et outils de l'assureur	**Par l'agent**
Transparence et perception des personnes concernées	**L'agent se présente en qualité de mandataire de l'assureur**	**L'agent ne se présente pas en qualité de mandataire de l'assureur**
	Conclusion L'assureur est le responsable du traitement et l'agent général le sous-traitant	**Conclusion** L'agent est le responsable du traitement

Mandataire d'assurance et Assureur

Relation Contractuelle	Mandat donné par l'assureur au mandataire d'assurance
Traitement nécessitant des données personnelles	✎ Ensemble des traitements répondant aux finalités passation, gestion et exécution des contrats d'assurance dans le cadre du mandat ✎ Ensemble des traitements répondant aux finalités de prospection commerciale dans le cadre du mandat
Détermination des finalités	**Par l'assureur**
Détermination des moyens essentiels	**Par l'assureur**
Détermination des moyens non-essentiels	**Par l'assureur**
Degré de contrôle	**Par l'assureur** Instructions précises et outils de l'assureur
Transparence et perception des personnes concernées	**La marque de l'assureur est prépondérante**

Conclusion
L'assureur est le responsable de traitement
et le mandataire d'assurance est le sous-traitant

Coassureurs

Relation Contractuelle	Convention de coassurance
Traitement nécessitant des données personnelles	✎ Passation, gestion et exécution des contrats d'assurance ✎ Lutte contre la fraude / LCB-FT ✎ Opérations de prospection
Détermination des finalités	**Par chacun des assureurs indépendamment des autres**
Détermination des moyens essentiels	**Par chacun des assureurs indépendamment des autres**
Détermination des moyens non-essentiels	**Par chacun des assureurs indépendamment des autres**
Degré de contrôle	**Par chacun des assureurs indépendamment des autres** **Les engagements contractuels et les traitements sont distincts**
Transparence et perception des personnes concernées	**Par chacun des assureurs indépendamment des autres**

Conclusion
Chaque assureur est responsable du traitement pour le traitement concernant sa part de couverture du risque

Réassureur et assureur

Relation Contractuelle	Contrat de réassurance
Traitement nécessitant des données personnelles	✎ Passation, gestion et exécution des traités de réassurance ✎ Lutte contre la fraude / LCB-FT
Détermination des finalités	**Par le réassureur**
Détermination des moyens essentiels	**Par le réassureur**
Détermination des moyens non-essentiels	**Par le réassureur**
Degré de contrôle	**Par le réassureur**
Transparence et perception des personnes concernées	**La marque de l'assureur est prépondérante**

Conclusion
Chacun est responsable de son propre traitement

Assureur et expert

Relation Contractuelle	Convention d'expertise
Traitement nécessitant des données personnelles	Conduite de l'expertise
Détermination des finalités	**Par l'expert ou l'assureur**
Détermination des moyens essentiels	**Par l'expert** lorsqu'il met en œuvre ses méthodes spécifiques ou **par l'assureur** lorsqu'il encadre la procédure d'expertise
Détermination des moyens non-essentiels	**Par l'expert**
Degré de contrôle	**L'expert est indépendant**
Transparence et perception des personnes concernées	**La marque de l'assureur est prépondérante ou notoriété de l'expert prépondérante**

Conclusion

En principe l'expert est le responsable du traitement.

Dans certaines hypothèses, lorsque la mission de l'expert est fortement encadrée, l'assureur peut être considéré comme le responsable du traitement et l'expert est le sous-traitant.

(La qualité de sous-traitant au sens du RGPD ne remet en aucun cas en cause l'indépendance de l'expert).

2

Finalités et bases légales des traitements

Pour être conformes au RGPD, les traitements de données personnelles doivent notamment avoir une finalité déterminée et une base légale.

Spécifiquement dans le secteur de l'assurance, les données peuvent être traitées pour la passation, gestion et l'exécution des contrats d'assurance (Finalité 1) ou pour la prospection commerciale par les Organismes d'assurance (Finalité 2).

- **Pour la passation, gestion et exécution des contrats d'assurance** (Finalité 1), la plupart des traitements ont comme base légale « l'exécution du contrat » (article 6, 1°, b) du RGPD). L'intérêt légitime de l'organisme d'assurance (article 6, 1°, f) du RGPD) ou le respect d'une obligation réglementaire (article 6, 1°, c) du RGPD) peuvent également fonder les traitements de données de cette finalité. En outre, le traitement des données de santé nécessite le respect de conditions particulières (article 9, 2°) du RGPD) (voir infra : Catégories de données personnelles et utilisation des données de santé)

- **Pour les opérations de prospection commerciale** (Finalité 2), les traitements ont comme base légale, l'intérêt légitime de l'Organisme d'assurance (article 6, 1°, f) ou le consentement s'agissant de la prospection par voie électronique (article L. 34-5 du Code des postes et communications électroniques).

Les tableaux, ci-dessous, listent les catégories de traitements de données personnelles mis en œuvre par les organismes d'assurance.

Finalité 1 : Passation, gestion et exécution des contrats d'assurance[14]

Base légale : Nécessaire à l'exécution d'un contrat auquel la personne concernée est partie[15] ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci (article 6, 1°, b) du RGPD).

Traitements que cela regroupe :

Étude des besoins spécifiques de chaque assuré éventuel afin de proposer des contrats adaptés[16]

Il s'agit de l'étude des besoins de l'assuré éventuel, à sa demande, dans le cadre du respect de l'obligation de conseil du distributeur d'assurance. Cette obligation nécessite d'une part, de préciser les exigences et besoins de l'assuré éventuel, et d'autre part, les raisons justifiant le conseil donné pour un produit d'assurance déterminé.
En assurance vie, le responsable de traitement doit en outre, s'enquérir auprès de l'assuré éventuel de sa situation financière et de ses objectifs d'investissement, ainsi que de ses connaissances et de son expérience en matière financière.

Examen, acceptation, contrôle et surveillance du risque

Il s'agit de « l'appréciation des risques assurantiels ». Cela comprend notamment l'examen et l'évaluation des caractéristiques du risque pour en déterminer une tarification et vérifier son assurabilité, y compris au moyen de profilages. Pour rappel : tout 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 conformément au droit des assurances[17].

Exécution des garanties des contrats

Il s'agit des opérations techniques nécessaires à la mise en œuvre des garanties et des prestations (établissement des préjudices, établissement du montant de l'indemnisation). Dans ce cadre, les données collectées sont relatives à la gestion des prestations et à la gestion des sinistres.

Gestion des contrats

Il s'agit de l'émission et de la preuve de la fourniture des documents précontractuels et contractuels, des opérations relatives à l'appel et au règlement des primes ou cotisations et de l'émission et la conservation des documents

[14] **Pour la passation :** Il s'agit notamment 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, qui rend nécessaire de préciser les exigences et les besoins du souscripteur éventuel ainsi que les raisons qui motivent le conseil fourni quant à un produit d'assurance déterminé, Cela concerne aussi « *l'examen, l'acceptation, le contrôle et la surveillance du risque* ». Ces termes sont plus généralement englobés dans le terme de l'appréciation des risques. L'appréciation du risque 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, établir la tarification et vérifier l'assurabilité.

Pour la gestion : 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. Il s'agit également de toute la relation clientèle, programme de fidélité…

Pour l'exécution : Il s'agit notamment des opérations nécessaires à la mise en œuvre des garanties et des prestations, la gestion des contentieux, le respect d'obligations légales…

[15] En assurance, la notion de partie au contrat doit s'entendre de toute personne partie, intéressée ou intervenant au contrat

[16] Outre l'utilisation de l'article 6, 1° b du RGPD comme base légale, l'article 6, 1° c du RGPD peut également constituer une base légale au devoir de conseil. L'Organisme d'assurance est soumis au respect d'une obligation légale qui figure aux articles L521-4 du Code des assurances (pour l'assurance non-vie) et L522-5 du Code des assurances (pour l'assurance vie). Également, le Règlement délégué du 21/09/2017 complétant la Directive (UE) 2016/97 (concernant les exigences en matière d'information et les règles de conduite applicables à la distribution de produits d'investissement fondés sur l'assurance) impose aux distributeurs de collecter un certain nombre de données telles que la situation financière du client (informations sur la source et l'importance de ses revenus réguliers, ses actifs, ses biens immobiliers…), ses connaissances et son expérience en matière financière.

[17] Article R. 336-1 e) du Code des assurances.

comptables y afférents, des modifications subséquentes de garantie en cours de contrat amenant à l'émission d'avenants, des opérations de répartition éventuelle entre les coassureurs et les réassureurs, du commissionnement, de la surveillance des risques, et des autres opérations techniques.

Gestion des clients

Il s'agit des traitements concernant :
-le regroupement des contrats et pièces pour un même client au sein de l'entreprise ou de la mise à jour des informations clients ;
-la gestion d'opérations techniques (ce qui inclut par exemple : les opérations techniques comme la normalisation et la suppression des doublons).

Gestion des réclamations et contentieux

La gestion des réclamations correspond aux situations où l'assuré conteste une décision ou absence de réaction de l'organisme d'assurance. Il s'agit de traitements qui interviennent dans le cadre des contentieux liés au contrat d'assurance et qui permettent notamment à l'entreprise d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou la défense des personnes concernées, ou de traiter les réclamations conformément aux procédures de médiation. Les traitements de données relatifs à des contentieux ayant pour objet l'application des contrats ont pour base légale l'exécution du contrat d'assurance.

Exercice des recours

L'exercice des recours correspond notamment aux situations où l'assureur qui a indemnisé son assuré, se retrouve subrogé dans ses droits et peut alors se retourner contre le responsable du dommage.

Base légale : Nécessaire aux fins des intérêts légitimes poursuivis par l'organisme d'assurance (article 6, 1°, f) du RGPD)

Traitements que cela regroupe :

Élaboration des statistiques et études actuarielles

Tous les contrats sont souscrits en appliquant une politique de souscription définie par les instances d'administration et de gestion de chaque organisme d'assurance. Ces règles sont fixées par la directive solvabilité 2 du 25 novembre 2009 et son règlement délégué du 10 octobre 2014. Ces obligations prudentielles sont notamment indiquées aux articles 48 (fonction actuarielle), 77, 84 et 121[19]. Ainsi par exemple, l'article 84 dispose que sur demande des autorités de contrôle, les entreprises d'assurance et de réassurance démontrent le caractère approprié du niveau de leurs provisions techniques, ainsi que l'applicabilité et la pertinence des méthodes qu'elles appliquent et l'adéquation des données statistiques sous-jacentes qu'elles utilisent.

Des études statistiques et actuarielles doivent être réalisées pour se conformer à ces obligations prudentielles afin de justifier que les engagements contractuels des organismes des assureurs sont compatibles avec leur solvabilité.

Le pilier I de Solvabilité II regroupe les exigences quantitatives, c'est-à-dire les règles de valorisation des actifs et des passifs, ainsi que les exigences de capital et leur mode de calcul[20].

Le pilier II de Solvabilité II regroupe d'une part les exigences qualitatives, en premier lieu les règles de gouvernance et de gestion des risques, et d'autre part l'évaluation propre des risques de la solvabilité (Own Risk and Solvency Assessment - ORSA).

[18] **Normalisation** : Remettre les adresses postales ou courriel aux normes en vigueur
Dédoublonnage : Supprimer les doublons dans un même fichier
Déduplication : Supprimer les doublons dans plusieurs fichiers

[19] Certaines références à la directive solvabilité peuvent être remplacées ou complétées par des références ayant le même objet dans le Code des assurances du fait de la transposition. Exemple avec l'article R.351-13 : les entreprises d'assurance et de réassurance doivent mettre en place des processus et procédures internes de nature à garantir le caractère approprié, l'exhaustivité et l'exactitude des données utilisées dans le calcul de leurs provisions techniques prudentielles mentionnées à l'article L. 351-2.

[20] Solvabilité II prévoit deux exigences de capital :
• le minimum de capital requis (Minimum Capital Requirement – MCR en anglais) ;
• le capital de solvabilité requis (Solvency Capital Requirement – SCR en anglais).
Le SCR peut être calculé au moyen d'une formule standard prévue par la directive Solvabilité II et le règlement délégué de la Commission européenne du 10 octobre 2014 ou d'un modèle interne complet ou partiel (certains risques étant alors couverts par la formule standard).

Par ailleurs, des paramètres propres à l'organisme (Undertaking Specific Parameters – USP en anglais) ou au groupe (Group Specific Parameters – GSP) peuvent remplacer certains paramètres de la formule standard.

Dans ce cadre, l'EIOPA a notamment pour mission de fournir régulièrement certaines informations techniques nécessaires à la valorisation du bilan Solvabilité II et au calcul du SCR, notamment :
• l'ajustement symétrique pour le sous-module « Actions » du risque de marché ;
• les courbes des taux sans risque de base par monnaie ;
• les corrections pour volatilité (volatility adjustment – VA) par monnaie et par pays ;
• les marges fondamentales par monnaie pour le calcul de l'ajustement égalisateur (matching adjustment – MA).

Il comprend :

- La gouvernance dans Solvabilité II[21]
- L'ORSA[22]

Le pilier 3 de Solvabilité II concerne la communication d'informations au public et aux autorités de contrôle. Il vise à harmoniser au niveau européen les informations publiées par les organismes d'assurance ainsi que celles remises aux superviseurs[23].

Mise en place d'actions de prévention proposées par l'assureur

Afin d'éviter des sinistres ou de diminuer l'ampleur des sinistres. Il s'agit notamment d'alertes en cas de survenance de catastrophes naturelles ou d'intempéries, pour mettre en garde les assurés, leur indiquer les bons gestes à avoir.

En assurance automobile, il peut s'agir notamment d'alerter les assurés en cas de ralentissement sur les routes, verglas.

Pour les contrats MRH, il peut s'agir d'actions de sensibilisation pour la mise en place de mesure préventive pour éviter les risques d'incendie, d'explosion, d'intoxication.

Pour les acteurs de la protection sociale, il peut s'agir d'actions de préventions concernant la santé ou de sensibilisation en matière d'action sociale, notamment à destination des aidants.

Conduite d'activités de recherche et développement

Il s'agit notamment des traitements ayant pour but d'améliorer l'ensemble des produits et services en dehors de la procédure prévue pour les recherches dans le cadre du Health Data Hub (article 41 de la loi relative à l'organisation et à la transformation du système de santé – juillet 2019).

Elle n'a pas pour objectif de modifier individuellement les droits contractuels des personnes. Il s'agit par exemple d'aider à améliorer les process de gestion des contrats (ex : réduction du nombre de pièces à fournir...).

[21] La gouvernance dans Solvabilité II renforce les règles de gouvernance et de gestion des risques des organismes d'assurance.

Le niveau 1
La directive Solvabilité II, modifiée par Omnibus 2 (version consolidée de la directive publiée par la Commission européenne), fixe les principes de gouvernance.
Les dispositions relatives à la gouvernance de la directive ont été transposées d'une part par l'ordonnance de transposition de Solvabilité II du 2 avril 2015 et d'autre part par le décret du 7 mai 2015 pris pour l'application de l'ordonnance susmentionnée. La directive prévoit que certains principes soient précisés dans un règlement délégué, adopté le 10 octobre 2014 et en vigueur depuis le 18 janvier 2015. Le chapitre 9 est consacré au système de gouvernance.

Les textes de niveau 3
La directive et le règlement délégué sont complétés par deux types de textes dits de niveau 3.
Les normes techniques d'exécution (Implementing Technical Standards – ITS) sont proposées par l'EIOPA puis adoptés par la Commission européenne dans les trois mois suivant leur réception. Ils sont d'application directe.
Les orientations sont adoptées par l'EIOPA puis, au sein de chaque autorité nationale, soumises à une procédure dite de comply or explain. Les autorités nationales doivent en effet mettre en œuvre ces orientations pour leur marché, ou expliquer à l'EIOPA pourquoi elles ne le font pas.
Les projets d'ITS et d'orientations sur le pilier II ont été adoptés par l'EIOPA.
Les orientations sur le système de gouvernance ont été publiées en français le 14 septembre 2015. L'ACPR a déclaré à l'EIOPA être en conformité avec la quasi-totalité de ces orientations. Les tableaux de mise en conformité sont disponibles sur la page consacrée aux orientations de l'EIOPA.

[22] **L'ORSA est un processus interne d'évaluation des risques et de la solvabilité par l'organisme (ou le groupe).** Il doit illustrer la capacité de l'organisme ou du groupe à identifier, mesurer et gérer les éléments de nature à modifier sa solvabilité ou sa situation financière. Aussi, sa déclinaison opérationnelle fait de lui un outil stratégique de premier plan qui doit être appréhendé par l'organisme comme un outil de pilotage de l'activité en fonction des risques. L'ORSA est défini dans l'article R.354-3 (article 45 de la directive Solvabilité II). Il comporte obligatoirement trois évaluations :

- l'évaluation du besoin global de solvabilité ;
- l'évaluation du respect permanent des obligations réglementaires concernant la couverture du SCR, du MCR et des exigences concernant le calcul des provisions techniques ;
- l'évaluation de l'écart entre le profil de risque de l'entreprise et les hypothèses qui sous-tendent le capital de solvabilité requis.

L'article 262 du Règlement délégué apporte des précisions sur le Besoin Global de Solvabilité. Les orientations de l'EIOPA apportent des éléments utiles sur la réalisation de l'exercice. Elles sont reprises dans la Notice « Solvabilité II » - évaluation interne des risques et de la solvabilité (ORSA)

[23] **Le Pilier 3, relatif aux obligations de reporting au superviseur et de diffusion d'information au public, est un élément essentiel de la directive Solvabilité II.**
Dans ce cadre, l'harmonisation des formats de reporting à l'échelle de l'Union Européenne est essentielle pour assurer une mise en œuvre cohérente des cadres européens de réglementation et de supervision afin de soutenir l'objectif d'amélioration de l'efficacité et de la cohérence de la supervision des institutions financières à travers l'Europe.
La documentation complète sur le reporting Solvabilité 2 au niveau européen est consultable sur le site de l'EIOPA (« Full Solvency II Reporting »).
La consultation des questions-réponses (Q&A) sur les états quantitatifs européens est disponible ici (voir en particulier Q&A on the ITS on Reporting et Q&A on the Guideline for Financial Stability Reporting).

Les exigences nationales complémentaires :
Le reporting Solvabilité II fait l'objet d'une harmonisation maximale au niveau européen. Néanmoins, il peut être complété par des états nationaux spécifiques, qui sont cependant limités aux besoins non couverts par Solvabilité II et correspondant à des spécificités nationales de la réglementation ou du marché.

L'ACPR a ainsi défini des états nationaux spécifiques (ENS) correspondant à des besoins prudentiels (participation aux bénéfices, taux servi, assurance construction, RC médicale, etc.) et statistiques, ainsi que des états issus des annexes aux comptes statutaires en cours de définition par l'Autorité des normes comptables (ANC).

Ce jeu d'états peut être segmenté selon les sous-ensembles suivants :

- Des états prudentiels fondés sur des données issues des comptes individuels ;
- Un état prudentiel fondé sur des données Solvabilité II : suivi de l'activité de substitution ;
- Des états à caractère comptable reprenant des informations issues des comptes individuels et de leurs annexes ;
- Des états statistiques existants applicables à tous les organismes (prévoyance complémentaire et sur RC Médicale).

Opérations de communication et de fidélisation de la clientèle ou d'amélioration de la qualité du service

Il s'agit des traitements :

- relatifs aux programmes de fidélité ou jeux concours au sein d'une entité ou plusieurs entités juridiques ;
- relatifs à la connaissance des attentes des clients ou la réalisation d'enquêtes de satisfaction ou sondages.

Lutte contre la fraude

Le considérant (47) du RGPD prévoit que les intérêts légitimes d'un responsable du traitement, y compris ceux d'un responsable du traitement à qui les données à caractère personnel peuvent être communiquées, ou d'un tiers peuvent constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement. 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 circonstances où les personnes concernées ne s'attendent raisonnablement pas à un traitement ultérieur.

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 traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime.

La fraude peut être définie comme « t*out acte ou omission commis intentionnellement par une ou plusieurs personnes physiques ou morales afin d'obtenir un avantage ou un bénéfice de façon illégitime, illicite ou illégale*». Le traitement de lutte contre la fraude est consubstantiel à la gestion de l'exécution des contrats. Une suspicion de fraude peut survenir à la suite d'une anomalie constatée dans la gestion du contrat ou fait suite à des contrôles menés par l'assureur. Elle est donc indissociable des activités de gestion des contrats d'assurance.

Ces traitements relatifs à la lutte contre la fraude concernent :

- l'analyse et la détection des actes réalisés dans le cadre de la passation, la gestion et l'exécution des contrats présentant une anomalie, une incohérence, ou ayant fait l'objet d'un signalement pouvant révéler une fraude à l'assurance,
- la gestion des alertes en cas d'anomalies, d'incohérences ou de signalements,
- la constitution de listes des personnes dûment identifiées comme auteurs d'actes pouvant être constitutifs d'une fraude,
- la gestion des procédures amiables, contentieuses, et disciplinaires consécutives à un cas de fraude,
- l'exécution des dispositions contractuelles, législatives, réglementaires ou administratives en vigueur applicables consécutivement à une fraude.

Ces traitements permettent de prévenir, de détecter ou de gérer les opérations, actes, ou omissions présentant un risque de fraude et émanant soit:

- pour la fraude externe : des personnes parties, intéressées ou intervenant au contrat;
- pour la fraude interne : des personnels salariés, des prestataires, des agents généraux, des mandataires, des intermédiaires, des administrateurs, mandataires sociaux, ou des élus des organismes. Des requêtes individuelles et ponctuelles peuvent être effectuées par l'employeur, dans le cadre de son pouvoir d'enquête interne, sur les données collectées au titre de la gestion administrative du personnel.

Les destinataires des données à caractère personnel dans le cadre de la lutte contre la fraude, sont visés en page 65 du présent guide.

Sur l'organisation interne des organismes d'assurance, il existe classiquement trois niveaux de contrôle. Les organismes d'assurance habilitent des gestionnaires à la lutte contre la fraude. En

général, ces gestionnaires dépendent d'une cellule de contrôle, distincte des services de gestion en charge de la passation ou de l'exécution des contrats. Il faut souligner que l'ensemble des personnes étant habilitées à traiter de la fraude ont reçu des formations appropriées, et sont soumis à une obligation de confidentialité dans le traitement des données.

Aucune décision produisant des effets juridiques à l'égard des personnes concernées par des données traitées dans le cadre de la lutte contre la fraude à l'assurance ne peut être prise sur le seul fondement de traitements automatisés.

Dès lors, les requêtes ou alertes détectées automatiquement doivent donner lieu à une analyse non automatisée par le personnel habilité du responsable de traitement ou du groupe auquel il appartient, le cas échéant des investigations complémentaires pourront être diligentées.

Enfin, la personne concernée doit être mise en mesure de présenter ses observations si une décision produisant des effets juridiques est prise à son égard dans le cadre de la conclusion ou de l'exécution d'un contrat.

Gestion du client intra groupe

Le regroupement des contrats et pièces pour un même client au sein du groupe d'assurance, ou de la mise à jour des informations clients. L'efficacité de la gestion administrative des contrats peut nécessiter et justifier le regroupement au niveau du groupe d'assurance, des données d'identification et de coordonnées. Les contrats de différentes sociétés d'un même groupe peuvent en effet être complémentaires et peuvent constituer une couverture adaptée aux besoins d'assurance du client. La réponse aux besoins d'assurance peut se traduire par la prise en compte de certaines données pour plusieurs contrats d'entités différentes d'un même groupe.

Cette possibilité de se fonder sur l'intérêt légitime pour regrouper des données administratives d'un même client au sein d'un groupe, est donc soumise à la réalisation préalable d'une balance des intérêts satisfaisante.

Base légale : Nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (article 6, 1°, c) du RGPD)

Traitements que cela regroupe :

Tout traitement imposé par la législation en vigueur

Il s'agit notamment du prélèvement à la source de l'impôt sur le revenu, de la lutte contre le blanchiment des capitaux et le financement du terrorisme, le respect des sanctions économiques et financières internationales...

Finalité 2 : Prospection commerciale par les Organismes d'assurance

Lorsque la prospection commerciale est réalisée à destination d'un particulier :

• par voie postale ou par appels téléphoniques ;

• ou par voie électronique lorsqu'il est déjà client pour des biens et services analogues à ceux déjà fournis.

Lorsque la prospection commerciale est réalisée à destination d'un professionnel

Base légale : Intérêt légitime de l'Organisme d'assurance (article 6, 1°, f) du RGPD) sous réserve d'une information préalable claire et de la possibilité pour les personnes de s'y opposer préalablement et à tout moment.

Traitements que cela regroupe :

Effectuer les opérations relatives à la gestion des prospects de l'Organisme d'assurance

Il s'agit notamment :

- de la gestion d'opérations techniques (ce qui inclut notamment les opérations techniques comme la normalisation, l'enrichissement et la déduplication) ;
- de la sélection de personnes pour réaliser des actions de fidélisation, de prospection, de sondage, de test produit ou services et de promotion ;
- des opérations de parrainage ;
- l'organisme d'assurance peut être amené à tester un nouveau produit d'assurance ou un service associé auprès d'un panel de prospects (par exemple, test d'un nouveau produit d'assurance auprès de résidents d'un département, test d'un contrat « chien-chat » auprès d'associations de protection des animaux) ;
- des jeux concours peuvent être également mis à disposition des prospects (par exemple : permettre de gagner un détecteur de fumée, des objets publicitaires, une invitation à un événement organisé par le responsable de traitement…) ;
- de la réalisation d'opérations de sollicitations ;
- de l'élaboration de statistiques commerciales ;
- de la gestion des avis des personnes sur des produits, services ou contenus.

L'acquisition, la cession, la location ou l'échange des données relatives à l'identification des prospects de l'Organisme d'assurance

Ces traitements visent à améliorer le service au client en proposant des produits ou services permettant de réduire la sinistralité ou de proposer un contrat ou une prestation complémentaire. Par exemple, et dans un objectif de prévention, les assureurs peuvent être amenés à céder des fichiers de clients victimes de vol à des partenaires spécialisés en télésurveillance.

Lorsque la prospection commerciale est réalisée à destination d'un particulier :
• par voie électronique (en vue de l'envoi de courriel, SMS, automate vocal, etc.)

Base légale : Consentement (article L. 34-5 du Code des postes et communications électroniques) sauf exceptions notamment si la prospection est à destination d'un client et concerne des produits ou services analogues.

Traitements que cela regroupe :

Effectuer les opérations relatives à la gestion des prospects de l'Organisme d'assurance

Les opérations de traitement sont les mêmes que pour la prospection par voie postale ou par appel téléphonique pour les consommateurs ou à destination de professionnels (voir supra)

L'acquisition, la cession, la location ou l'échange des données relatives à l'identification des prospects de l'Organisme d'assurance

Les opérations de traitement sont les mêmes que pour la prospection par voie postale ou par appel téléphonique pour les consommateurs ou à destination de professionnels (voir supra)

Gestion des listes d'opposition à recevoir de la prospection

Tout organisme mettant en œuvre une prospection commerciale par voie téléphonique doit retirer de sa liste les personnes inscrites sur la liste d'opposition prévue par les dispositions des articles L. 223-1 et suivants du code de la consommation (liste dite « BLOCTEL ») sans préjudice des exceptions légales.

3

Profilage et décisions individuelles automatisées

Profilage

Le profilage est défini par le RGPD comme : « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique* ».

Pour mettre en œuvre les finalités précitées, les responsables de traitement peuvent avoir recours au profilage tel qu'il est défini à l'article 4, 4° du RGPD.

La qualification de profilage au sens du texte précité peut être retenue en l'absence de traitement entièrement automatisé, dès lors que ce moyen de traitement conduit à une évaluation des caractéristiques individuelles d'une personne physique (évaluer certains aspects personnels en vue d'émettre un jugement ou de tirer des conclusions sur elle).

Le profilage n'est jamais, en tant que tel, une finalité mais seulement un moyen à disposition des organismes d'assurance. Cela est, par exemple, le cas dans le cadre de la finalité passation, gestion et exécution des contrats d'assurance où le profilage implique l'évaluation des caractéristiques du risque assurantiel pour en déterminer la fréquence, le coût moyen, le coût du sinistre maximum possible, la tarification et vérifier l'assurabilité du risque.

Les conditions d'acceptation et les conditions tarifaires sont fixées dans le cadre de la politique d'acceptation des risques établie conformément à la réglementation assurantielle en vigueur à partir notamment de critères actuariels, environnementaux ou comportementaux.

Lorsque l'organisme d'assurance a recours au profilage, il doit en indiquer l'existence dans les mentions d'information. Les personnes doivent comprendre la finalité exacte du profilage et l'usage qui est fait de leurs données, c'est-à-dire avoir connaissance de l'origine de celles-ci et de leurs croisements éventuels.

En outre, les droits d'accès, de rectification, de limitation et d'effacement s'exercent non seulement sur les données qui ont contribué à la construction d'un profil mais également sur le profil en lui-même

La personne concernée peut, de manière discrétionnaire et à tout moment, s'opposer à un profilage dont la finalité est la prospection (art 21-2 RGPD), elle peut également exercer son droit d'opposition lorsque la base légale est l'intérêt légitime (art 21-1 RGPD).

Décision individuelle automatisée, y compris le profilage (article 22 du RGPD)

Le responsable de traitement peut également avoir recours à des décisions individuelles automatisées, c'est-à-dire des décisions :

- fondées exclusivement sur un traitement automatisé ;
- qui produisent des effets juridiques ou des effets similaires à l'égard de la personne concernée (la publicité ciblée qui est basée sur le profilage ne produit, en principe, pas d'effets juridiques ou similaires à l'égard des personnes, ce traitement n'est donc pas considéré systématiquement comme une décision individuelle automatisée). Par exemple, la décision impacte la situation financière de la personne (par exemple, l'application de tarifs plus élevés).

Le recours à ce type de décision est possible dès lors que cela est :

- nécessaire à la conclusion ou à l'exécution du contrat d'assurance ;
- ou autorisé par une disposition légale ou réglementaire ;
- ou fondé sur le consentement explicite de la personne concernée.

De telles décisions ne peuvent être fondées sur les catégories particulières de données visées à l'article 9 du RGPD que si l'assuré a donné son consentement explicite pour le traitement des données particulières ou lorsque le traitement est nécessaire pour des motifs d'intérêt public[24].

Le recours à ce type de décision peut permettre d'accélérer les démarches des personnes concernées.

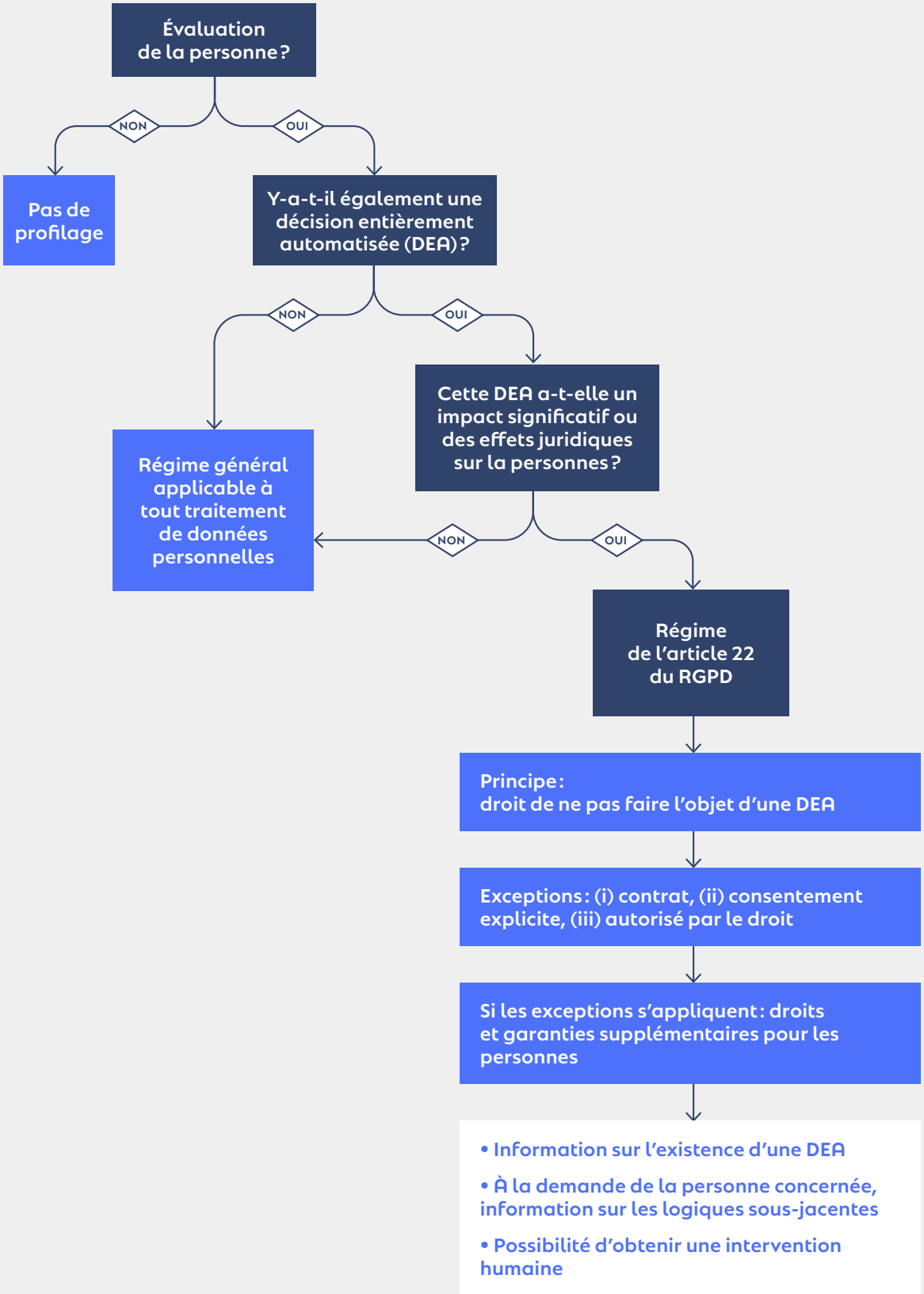
S'il a recours à des décisions individuelles automatisées, y compris le profilage, dans les conditions de l'article 22 du RGPD, le responsable de traitement doit prévoir des garanties supplémentaires :

- il doit notamment permettre à la personne concernée d'obtenir une intervention humaine, par exemple, en lui donnant la possibilité de contacter une personne ayant la capacité de revoir la décision (le gestionnaire du contrat par l'intermédiaire du service client), d'exprimer son point de vue, d'obtenir une explication sur la décision prise ;
- les personnes doivent être informées, lors de la collecte de leurs données et à tout moment sur leur demande, de l'existence d'une telle décision, de la logique sous-jacente ainsi que de l'importance et des conséquences prévues de cette décision.

En outre, le responsable de traitement doit communiquer à la personne concernée, si elle en fait la demande au titre de son droit d'accès, les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre, à l'exception des secrets protégés par la loi tels que le secret des affaires et la propriété intellectuelle.

[24] Pour rappel, la collecte des données de santé n'est pas autorisée au regard de l'exception des dispositions de l'article 9.2.g du RGPD relatif aux motifs d'intérêt public importants.

Synthèse décision entièrement automatisée



4

Catégories de données à caractère personnel traitées

Dans le cadre des deux finalités énoncées précédemment, les responsables de traitement traitent les données suivantes uniquement lorsqu'elles sont pertinentes et strictement nécessaires au traitement.

Pour un type de contrat donné, toutes les catégories de données citées ci-dessous ne sont pas nécessaires. Par exemple, pour la passation, la gestion ou l'exécution d'un contrat d'assurance complémentaire santé, les données relatives à la localisation du bien assuré ne sont pas nécessaires. A contrario, pour un contrat d'assurance habitation, responsabilité civile, les données relatives à la situation familiale sont nécessaires au contrat pour connaître le nombre de personnes dans le foyer.

La liste de données traitées pour les finalités 1 et 2, ci-après, est indicative.

Pour la passation, gestion et éxécution des contrats d'assurance (Finalité 1)

Les données d'identification

Les données relatives à l'identification des personnes parties, intéressées ou intervenantes au contrat sont notamment les éléments relatifs à :
- à l'état civil ;
- aux coordonnées ;
- 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. La nationalité est l'une des informations qui permet de déterminer quelles sont les éventuelles obligations notamment fiscales à l'égard de l'Etat dont le souscripteur est un ressortissant.

Les données relatives à la gestion du contrat

Il s'agit des données liées au contrat : le numéro d'identification du client, de l'assuré, du contrat, du dossier sinistre, les créances en cours, les références de l'apporteur, des coassureurs et des réassureurs, la durée, les montants, 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…

Les données relatives à la situation familiale

La situation familiale comprend notamment les éléments relatifs :
- à la situation matrimoniale (mariage, pacs, vie maritale…) ;
- à la composition du foyer (nombre de personnes composant le foyer, âge…) ;
- à la capacité et au régime de protection (minorité, tutelle, curatelle…).

Les données relatives à la situation économique, patrimoniale et financière

Les données relatives à la situation économique, financière et patrimoniale sont notamment les éléments relatifs :
- aux revenus du travail et autres revenus ;
- au patrimoine mobilier et immobilier ;
- aux encours et à l'endettement ;
- aux avoirs financiers ;
- aux données d'imposition ;
- aux crédits ;
- au capital souscrit/remboursé ;
- à la situation de surendettement ou d'ouvrant droit à avantages assurantiels - bénéficiaires CMU- ACS, RSA…
- à la composition du foyer fiscal

Les données nécessaires au paiement de la prime d'assurance

Il s'agit peut s'agir du :
- du numéro de chèque ;
- du numéro de carte bancaire, de la date de fin de validité de la carte bancaire dans le cadre de délibération n°2017-222 du 20 juillet 2017 de la CNIL ;
- des références bancaires (RIB / IBAN).

Les données relatives à la situation professionnelle

Les données relatives à la situation professionnelles sont notamment 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

Il s'agit notamment de la situation géographique, des caractéristiques du logement ou du local, des conditions d'occupation, des renseignements sur les biens assurables, le type et les (caractéristiques) du ou des biens.
Les informations relatives à la sinistralité et les antécédents de conduite et d'assurance, au permis de conduire, à la validité du permis de conduire et, le cas échéant, si le bien est utilisé sur le lieu de travail et lors de déplacements professionnels, aux éléments entraînant une déchéance de garantie…

Les données relatives à la détermination ou à l'évaluation des préjudices et des prestations

Il s'agit notamment :
- des données liées au sinistre : la nature et les circonstances du sinistre, la description des atteintes aux biens et/ou aux personnes, les PV de gendarmerie et autres rapports d'enquête, les rapports d'expertise, les éléments afférents aux procédures administratives ou judiciaires éventuellement engagées ;
- des données liées aux victimes : la nature et l'étendue des préjudices subis, le taux invalidité/incapacité, les rentes, le capital décès, les montants des prestations, données permettant de déterminer les obligations fiscales de la personne concernée, 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 données issues de pages internet ouvertes au public pour la recherche des bénéficiaires des contrats en déshérence.

Les données de géolocalisation des personnes ou des biens en relation avec les risques assurés ou les services proposés

Ces données sont notamment la position du véhicule assuré lorsque cela entre dans les conditions de mise en œuvre du contrat d'assurance.

Les données relatives aux habitudes de vie et aux usages des biens en relation avec les risques assurés ou les services proposés

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 aux usages des biens sont notamment les données nécessaires pour les contrats d'assurance véhicule professionnel, personnel, résidence principale et résidence secondaire, présence d'animaux domestiques.

Les données visées à l'article 9 du RGPD

Le RGPD n'autorise le traitement des données visées à l'article 9 que dans les conditions listées à l'article 9, 2° du RGPD. Ainsi :

❶ L'article 9 point b) du paragraphe 2 du RGPD peut s'appliquer aux Organismes d'assurance aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit de la protection sociale, à condition que le traitement soit autorisé par le droit de l'Union ou le droit français. Il s'agit des contrats relevant de ce périmètre, tels que :
- les contrats de complémentaire santé ;
- les contrats de prévoyance complémentaire ;
- la retraite supplémentaire ;
- l'assurance des risques statutaires.

❷ L'article 9 point a) du paragraphe 2 relatif au consentement peut être utilisé dès lors que le traitement des données de santé est « *nécessaire à l'exécution d'un contrat, y compris la fourniture d'un service* » si cette exécution est subordonnée au consentement explicite. Cela concerne :
- l'assurance emprunteur ;
- la prévoyance individuelle ;
- l'assistance[25] ;
- les contrats d'individuelle accident ;
- la protection juridique ;
- les garanties de Responsabilité civile ;
- les contrats obsèques.

❸ Le traitement de ces données est également possible :
- pour la constatation, l'exercice ou la défense d'un droit en justice (ex : action directe en RC) (article 9 (2) (f) du RGPD ;

dès lors que la personne concernée est dans l'impossibilité de consentir (ex : assistance) (article 9 (2) (c) du RGPD).

Le NIR

Le NIR peut être utilisé par les organismes d'assurance dans les conditions prévues par le décret du 19 avril 2019[26] (cf. en détail ci-dessous)

[25] Au sens de l'article R 321-1 du Code des assurances : « L'agrément administratif prévu par l'article L. 321-1 est accordé par l'Autorité de contrôle prudentiel. Pour l'octroi de cet agrément, les opérations d'assurance sont classées en branches et sous-branches de la manière suivante […]. Assistance aux personnes en difficulté, notamment au cours de déplacements ».

[26] Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire

[27] Conseil d'État, 10ème - 9ème chambres réunies, 06/04/2018, 406664

[28] En matière d'assurance, la Cour de cassation a plusieurs fois rappelé que l'atteinte à la vie privée de l'assuré causée par des opérations de surveillance mises en œuvre par l'assureur sont licites lorsqu'elles sont proportionnées au regard de la nécessaire et légitime préservation des droits de l'assureur et des intérêts de la collectivité des assurés (ex : Cass 1re civ, 22 septembre 2016, 15-24.015)

Les données d'infraction

En application de la jurisprudence du Conseil d'état, les données d'infraction sont celles collectées dans le but d'établir l'existence ou de prévenir la commission d'infractions[27]. Les assureurs sont, d'une part, autorisés par le Code des assurances à collecter des données d'infractions (art A.121-1 à A.121-2), et d'autre part, les données pouvant être traitées pour établir l'existence d'une infraction suite à un dépôt de plainte ne sont pas mobilisées pour établir ou prévenir une infraction mais pour indemniser les victimes.

Les données relatives à la lutte contre la fraude

Outre, les données précédemment citées qui peuvent être collectées uniquement dans les conditions requises :

Les données de localisation et connexion : il s'agit des données en lien avec le dossier de fraude (vidéo, photographies et métadonnées). Ne sont pas concernées, les données de géolocalisation des salariés répondant à une finalité autre que la lutte contre la fraude. Les données de localisation sont celles qui figurent sur les enregistrements permettant d'horodater et de localiser l'objet de l'enregistrement. Par exemple, une photo envoyée par l'assuré dans le cadre du rapport d'enquête, identifie le lieu du sinistre et sa date. Ainsi, il est possible de constater si la date correspond ou non avec celle de la déclaration du sinistre.

Les données issues de pages internet ouvertes au public[28] : la consultation de ces pages n'est possible qu'à condition que la suspicion de fraude soit corroborée avec d'autres informations relatives à la personne concernée. La collecte doit être limitée aux seules informations concernant un éventuel fraudeur. La collecte doit être réalisée manuellement par un gestionnaire habilité et ne pas conduire à une collecte massive des données présentes sur ces pages internet ouvertes au public.

Les données collectées au titre de la gestion administrative du personnel uniquement dans le cadre de requêtes ponctuelles et individuelles consécutives à la détection d'une fraude. Par exemple : vérification de la présence, des absences, la téléphonie, la rémunération, le badgeage des salariés…

Les données relatives aux anomalies, incohérences et signalements pouvant révéler une fraude : Exemples d'anomalies ou incohérences :

- La remise de « faux » et « l'usage de faux » lors de la souscription du contrat ou au stade de son exécution (ex : fausse fiche de paie, fausse carte vitale ou faux justificatifs d'identité…),
- Une signature illisible pouvant constituer un indice de fraude qui devra être conforté par d'autres éléments,
- La répétition de plusieurs sinistres pour un même bien ou une même personne,
- plusieurs personnes impliquées pour des mêmes sinistres,
- une incohérence sur les dates indiquées,
- le refus de communication d'une information ou d'un justificatif,
- la modification récurrente d'un RIB ou quasiment concomitante avec la fraude,
- une période très courte entre la souscription du contrat d'assurance et la réalisation du sinistre,
- des modifications répétées des bénéficiaires d'une clause contractuelle ou quasiment concomitantes avec la fraude.

Les données relatives aux investigations, à l'instruction du dossier de fraude et à l'évaluation du périmètre de la fraude. Exemples de données de gestion d'un dossier de fraude :

- descriptif des anomalies, indicateurs, incohérences, alertes automatiques ou signalement ayant permis de détecter la fraude,
- investigations, instruction du dossier de fraude et évaluation : descriptif de la fraude, faits, personnes suspectées, témoins, dates, préjudice résultant de la fraude pour l'organisme ou les personnes victimes, rapports d'enquête, expertises, durée, montant, nombre de personnes impliquées, décisions prises par l'organisme,
- données issues des bases de données internes (bases relation client, gestion des contrats, gestion du personnel ou des intermédiaires…) ou de fichiers externes (Agira, Alfa, Argos…) ou encore de bases externes et registres qui sont destinés exclusivement à l'information du public et sont ouverts à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime.

Les données d'identification des personnes intervenant dans la détection et la gestion de la fraude. Exemple : les enquêteurs et les personnes impliquées dans l'enquête, dont l'usage de pseudonymes, ou identités fictives destinées à protéger ces personnes.

Pour la prospection commerciale de l'organisme d'assurance (Finalité 2)

Les données relatives à l'identification des personnes

Il s'agit notamment :

- des informations classiques : civilité, nom(s), prénoms, adresse, numéro de téléphone (fixe et/ou mobile), numéro de télécopie, adresses de courrier électronique, date de naissance ;
- pour l'identification du prospect : le code interne de traitement.

Les données relatives au suivi de la relation commerciale

Il s'agit notamment des demandes de documentation ou de renseignements, des demandes relatives aux produits, services ou abonnements proposés, les montants, la périodicité, les adresses, les données relatives aux produits, les contrats et services, l'origine de la demande, les échanges et commentaires des prospects, les remises consenties ou avantages.

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

Il s'agit notamment de la vie maritale, du nombre de personnes composant le foyer, le nombre et l'âge du ou des enfant(s) au foyer, la profession, le domaine d'activité, la présence d'animaux domestiques, les loisirs.

Les données relatives aux habitudes de vie en lien avec la relation commerciale

Les données relatives à la situation professionnelle et non professionnelles ayant un lien avec la relation commerciale

Les données du parcours digital

Il s'agit des dates et lieux de connexion sur les sites internet, applications mobiles, cookies, traceurs.

Les données relatives à la sélection de personnes pour réaliser des actions de fidélisation, de prospection, de sondage, de test produits et services et de promotion

Les données relatives à l'organisation et au traitement des jeux-concours, de loteries et de toute opération promotionnelle

Il s'agit notamment de la date de participation, les réponses apportées aux jeux-concours, la photographie ou l'image de la personne, et la nature des lots offerts.

Les données relatives aux contributions des personnes qui déposent des avis sur des produits, services ou contenus

Il s'agit notamment des pseudonymes.

5

Traitement du NIR

Le NIR peut être utilisé par les Organismes d'assurance dans les conditions prévues par le décret du 19 avril 2019[29].

❶ Dans le cadre de la protection sociale

L'article 2, A, 1°, b) autorise l'utilisation du NIR les organismes chargés de la gestion de l'assurance maladie complémentaire ou de la retraite complémentaire pour l'accomplissement de leurs missions en matière de protection sociale, y compris lorsque l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques est nécessaire pour la réalisation d'évaluations, d'études, de statistiques et de recherches, ou pour mettre en œuvre des échanges ou traitements intéressant plusieurs acteurs de la protection sociale.

❷ Pour la finalité la passation, la gestion et l'exécution des contrats d'assurance, de capitalisation, de réassurance ou pour leurs engagements de retraite

L'article 2, D, 15° du décret du 19 avril 2019 autorise l'utilisation du NIR, lorsque ce dernier est nécessaire aux traitements ayant pour finalité la passation, la gestion et l'exécution des contrats d'assurance, de capitalisation, de réassurance ou pour leurs engagements de retraite, par :

- les entreprises d'assurance ;
- les mutuelles et leurs unions ;
- les institutions de prévoyance et leurs unions ;
- les organismes de retraite professionnelle supplémentaire ;
- les entreprises de réassurance.

Cet article précise que ce traitement du NIR est uniquement possible pour :

- leurs activités d'assurance maladie, maternité, invalidité, retraite supplémentaire
- leurs activités d'assurance pour les garanties pertes d'exploitation et perte d'emploi uniquement à des fins probatoires ;
- les relations avec les professionnels, les établissements et les institutions de santé en vertu des dispositions du 3° de l'article R. 115-2 du Code de la sécurité sociale ;
- les déclarations sociales des entreprises souscriptrices de contrats d'assurance ;
- l'indemnisation des accidents de la circulation en vertu des articles R. 211-37 et R. 211-38 du Code des assurances ;
- la gestion des rentes en vertu des dispositions de l'article 39 A de l'annexe III du Code général des impôts et de l'article L. 81 A du livre de procédure fiscales ;
- l'exécution des dispositions légales, réglementaires et administratives en vigueur.

à l'exclusion de toute utilisation aux fins d'identification des doublons ou des homonymies.

[29] Décret n° 2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire.

A noter que le décret reprend les conditions d'utilisations du NIR telles que prévues par l'AU 31 - Délibération n° 2014-014 du 23 janvier 2014

Pour le prélèvement à la source

L'article 2, D, 5° du décret du 19 avril 2019 autorise le traitement du NIR par les employeurs, les organismes, les administrations et les services chargés de collecter l'impôt sur le revenu pour la mise en œuvre du prélèvement à la source prévu par l'article 204 A du Code général des impôts.

Pour la lutte contre la déshérence en assurance vie

L'article 2, D, 8° du décret du 19 avril 2019 autorise le traitement du NIR, pour la recherche des assurés, des adhérents, des souscripteurs ou des bénéficiaires de contrats d'assurance sur la vie ou de bons ou contrats de capitalisation décédés, par :

- les entreprises d'assurance ;
- les mutuelles et les unions ;
- les institutions de prévoyance et les unions ;
- les organismes de retraite professionnelle supplémentaire ;
- les entreprises de réassurance ;
- l'Association pour la gestion des informations et le risque en assurance (AGIRA).

L'article 2, D, 9° du décret du 19 avril 2019 autorise également le traitement du NIR, par l'AGIRA, pour la tenue de la base de données relative aux personnes dont le décès est connu de l'INSEE et la mise en place d'une plateforme informatique sécurisée permettant l'interrogation de cette base par les seuls organismes autorisés.

Pour la lutte contre le blanchiment de capitaux et le financement du terrorisme

L'article 2, D, 11° du décret du 19 avril 2019 autorise le traitement du NIR pour le respect des obligations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, et l'application des mesures de gel et d'interdictions de mise à disposition prévues par le Code monétaire et financier, uniquement dans l'hypothèse où le NIR figure sur les listes de gel des avoirs ou des sanctions financières, par les personnes mentionnées aux 1° à 7° de l'article L. 561-2 du Code monétaire et financier, parmi lesquels se trouvent :

- les entreprises d'assurance ;
- les mutuelles et les unions ;
- les institutions de prévoyance et les unions ;
- les organismes de retraite professionnelle supplémentaire ;
- les intermédiaires d'assurance définis à l'article L. 511-1 du Code des assurances sauf ceux qui agissent sous l'entière responsabilité de l'organisme ou du courtier d'assurance.

Pour la lutte contre la fraude

L'article 2, D, 14° du décret du 19 avril 2019 autorise le traitement du NIR, pour la lutte contre la fraude à l'assurance externe ou interne correspondant à un acte ou omission commis intentionnellement par une ou plusieurs personnes afin d'obtenir un avantage ou un bénéfice de façon illégitime, illicite ou illégale, par :

- les entreprises d'assurance ;
- les mutuelles et leurs unions ;
- les institutions de prévoyance et leurs unions ;
- les organismes de retraite professionnelle supplémentaire ;
- les entreprises de réassurance ;
- le fonds de garantie des assurances obligatoires de dommages, mentionné à l'article L. 421-1 du Code des assurances ;
- le fonds de garantie des victimes des actes de terrorisme et d'autres infractions, mentionné à l'article L. 422-1 du Code des assurances.

Il s'agit de :

- l'analyse et la détection des actes réalisés dans le cadre de la passation, la gestion et l'exécution des contrats présentant une anomalie, une incohérence, ou ayant fait l'objet d'un signalement pouvant révéler une fraude à l'assurance ;
- la gestion des alertes en cas d'anomalies, d'incohérences ou de signalements ;
- la constitution de listes des personnes dûment identifiées comme auteurs d'actes pouvant être constitutifs d'une fraude ;
- la gestion des procédures amiables, contentieuses, et disciplinaires consécutives à un cas de fraude.

6

Traitement des données de santé

Concernant la base légale des traitements des données de santé des organismes d'assurance, il est possible de retenir que[30] :

✎ L'article 9 point b) du paragraphe 2 du RGPD peut s'appliquer aux Organismes d'assurance aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit de la protection sociale. Il s'agit des contrats relevant de ce périmètre, tels que :

- les contrats de complémentaire santé ;
- les contrats de prévoyance complémentaire ;
- la retraite supplémentaire ;
- l'assurance des risques statutaires.[31]

✎ L'article 9 point a) du paragraphe 2 relatif au consentement[32] peut être utilisé dès lors que le traitement des données de santé est « *nécessaire à l'exécution d'un contrat, y compris la fourniture d'un service* » *si cette exécution est subordonnée au consentement explicite* ». Cela concerne :

- l'assurance emprunteur (ex : évaluation des risques pour proposer une tarification d'assurance) ;
- la prévoyance individuelle (ex : taux d'invalidité, dommages corporels subis) ;
- l'assistance[33] ;
- les contrats d'individuelle accident (ex : taux d'invalidité, dommages corporels subis) ;
- la protection juridique (ex : taux d'invalidité, dommages corporels subis) ;
- les garanties de Responsabilité civile (ex : taux d'invalidité, dommages corporels subis) ;
- les contrats obsèques.

✎ Le traitement de ces données est également possible :

- pour la constatation, l'exercice ou la défense d'un droit en justice (ex : action directe en RC) (article 9 (2) (f) du RGPD ;
- dès lors que la personne concernée est dans l'impossibilité de consentir (ex : assistance) (article 9 (2) (c) du RGPD).

[30] Cf. courrier de la Présidente de la CNIL en date du 29 janvier 2019

[31] En application de l'article 57 de la loi n°84-53 du 26 janvier 1984 la collectivité ou l'établissement verse des prestations dues à l'agent (traitement, et/ ou frais médicaux) en cas de maladie, maternité et adoption, accident décès, paternité. Une assurance peut être souscrite pour couvrir ces frais.

[32] A noter que lorsque la personne concernée est le souscripteur du contrat, son consentement ainsi que celui de son entourage (ex : membre de la famille) devra être donné au moment de la collecte de la donnée

[33] Au sens de l'article R321-1 du Code des assurances « Assistance aux personnes en difficulté, notamment au cours de déplacements. »

[34] Loi n° 89-1009 du 31 décembre 1989 renforçant les garanties offertes aux personnes assurées contre certains risques.

Outre les règles relatives aux bases légales offertes par l'article 9 du RGPD :

✎ L'utilisation des données de santé est très fortement encadrée par d'autres législations :

- En matière de complémentaire santé, à la souscription, pour être qualifié de solidaire et bénéficier du taux réduit de la taxe de solidarité additionnelle, le contrat ne doit pas prendre en considération l'état de santé de la personne. Par la suite, au cours de la vie du contrat, l'article 6 de la loi dite « Evin »[34] interdit toute modification individuelle du tarif du contrat en raison de l'évolution de l'état de santé de l'assuré. Dans ce domaine, le traitement des données de santé est donc requis uniquement pour le versement des prestations ;
- Pour tout contrat garantissant l'invalidité ou/et le décès ou pour les risques portant atteinte à l'intégrité physique de la personne, le Code pénal prévoit une exception au principe de non-discrimination fondée sur l'état de santé qui autorise les responsables de traitement à utiliser ce critère pour leurs opérations dans cette circonstance précise uniquement[35] ;
- En assurance emprunteur, la convention AERAS encadre le traitement des données personnelles nécessaires à la souscription et à l'exécution des contrats et notamment les modalités de questionnement[36] ;
- La directive 2009/138 dite solvabilité 2 et le règlement délégué 2015-35 du 10 octobre 2014 imposent aux organismes d'assurance un minimum de capital de solvabilité requis. Ce capital correspond au capital économique dont a besoin le responsable de traitement pour garantir sa solvabilité. Pour le calcul de ce capital, la directive prévoit que les modules de « risque de souscription en vie » doivent prendre en considération le taux d'invalidité, de maladie et de morbidité ainsi que l'état de santé de la personne assurée[37] ;
- Lorsqu'un contrat collectif à adhésion facultative relatif au remboursement ou à l'indemnisation des frais occasionnés par une maladie, une maternité ou un accident est coassuré par des organismes d'assurance régis par des codes différents, ces organismes coassureurs ne peuvent en aucun cas recueillir des informations médicales auprès des assurés du contrat ou des personnes souhaitant bénéficier d'une couverture, ni fixer les cotisations en fonction de l'état de santé[38].

Par ailleurs :

✎ Les données médicales sont couvertes par le secret professionnel ce qui implique l'intervention de professionnels de santé ou de personnes spécifiques soumises au secret professionnel agissant sous leur autorité et les traitements des données collectées sont alors réalisés dans le respect du code de bonne conduite annexé à la convention AERAS ;

✎ Le traitement des données génétiques par les responsables de traitement, ou peur leur compte, est interdit à la fois par le Code de la santé publique (article L. 1141-1 du Code de la santé publique), par les trois Codes assurantiels (article L. 133-1 du Codes des assurances, article L. 932-39 du Code de la sécurité sociale et article L. 110-6 du Code de la mutualité) et par le Code pénal (Article 225-3 du Code pénal).

[35] Article 225-3 du Code pénal

[36] Convention AERAS révisée

[37] Article 105, 3° de la directive 2009/138

[38] Article L. 145-2 du Code des assurances

7

Informations des personnes concernées

Le responsable du traitement doit fournir à la personne concernée les informations visées aux articles 13 et 14 du RGPD dans les conditions de l'article 12, ainsi que les informations supplémentaires prévues par l'ensemble des textes applicables aux traitements de données personnelles.

Modalités de l'information

Afin de répondre à l'ensemble de ces dispositions et dans un souci de bonne lisibilité pour la personne concernée, le responsable de traitement peut fournir distinctement, d'une part les informations pouvant être qualifiées d'« essentielles », et d'autre part, les informations « complémentaires ». Ces informations « complémentaires » peuvent être fournies par tout moyen approprié, et notamment par renvoi vers un document dédié sur le site internet du responsable de traitement.

Cette priorisation ne permet en aucun cas la transmission d'une information incomplète aux personnes concernées. Cela signifie que certaines informations « essentielles » sont particulièrement mises en avant, et qu'un accès simple et immédiat permet de consulter les autres informations.

Sous quel format ?

Ces informations sont fournies au format le plus adapté[39].

Lorsque ces informations sont fournies par écrit, elles peuvent l'être sur support papier ou par voie électronique.

Lorsque ces informations sont fournies à l'oral, notamment par voie téléphonique, la personne doit se voir indiquer comment accéder à une information complète par écrit.

Comment délivrer l'information ?

Ces informations doivent être fournies dans la mesure du possible de façon[40] :

- succincte ;
- clairement distincte des autres mentions d'informations du contrat ;
- adaptée au public visé ;
- concrète et explicite dans un langage simple et non technique ;
- facilement accessible.

Quand délivrer l'information ?

Lorsque le responsable de traitement obtient directement les données auprès de la personne concernée il doit au même moment lui fournir les informations.

Lorsque le responsable de traitement n'obtient pas directement les données de la personne concernée, il doit lui fournir les informations :

[39] Par exemple: sur papier, ou sur page internet

[40] Cf Guidelines on transparency under Regulation 2016/679, WP260 rev.01

- 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 ;
- 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 (ex : l'obligation d'information du bénéficiaire d'une assurance vie peut être retardée au moment où l'assureur l'avise de l'existence d'une stipulation effectuée à son profit).
- s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Cette fourniture n'est pas nécessaire quand :

- la personne concernée dispose déjà de ces informations (ex : pour les formulaires de versement en cours de contrat) ;

En outre, lorsque la collecte est indirecte, cette fourniture n'est pas nécessaire quand :

- la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés ou rend impossible/compromet gravement la réalisation des objectifs ;
- l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable de traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernées ;
- 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 membres, y compris une obligation légale de secret professionnel.

Mentions d'informations « essentielles » communes à tous les traitements

Les mentions d'informations « essentielles » communes à tous les traitements sont :

- L'identité et les coordonnées du responsable de traitement ;
- Le cas échéant, les coordonnées du délégué à la protection des données[41] ;
- Les finalités du traitement ;
- L'existence des droits ;
- Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ;
- L'existence du droit de retirer son consentement à tout moment lorsque le traitement a pour base légale le consentement.

Il peut être nécessaire d'ajouter une information essentielle pour les personnes concernées (exemples : prise de décision automatisée ou mise à disposition de données à des partenaires commerciaux).

Enfin, que la collecte soit directe ou indirecte, les modalités pour accéder aux informations complémentaires sont fournies au même moment que les informations « essentielles » (ex : renvoi vers le site internet de l'assureur ou vers un document).

Mentions d'informations « complémentaires » communes à tous les traitements

Les mentions d'informations « complémentaires » communes à tous les traitements sont :

- la durée de conservation des données ou les critères utilisés pour déterminer cette durée ;
- Lorsque le traitement est fondé sur l'intérêt légitime du responsable de traitement, l'information doit préciser quels sont les intérêts légitimes poursuivis ;
- Les destinataires ou catégories de destinataires[42] ;
- L'existence de transferts de données vers des pays hors de l'Union européenne ;
- L'existence d'une prise de décision automatisée, y compris un profilage ainsi que, à la demande de la personne concernée, les informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée et lorsque cela ne porte pas atteinte aux secrets des affaires ;
- des informations sur les autres finalités envisagées dès lors que le responsable de traitement a l'intention d'effectuer un traitement ultérieur des données pour une finalité distincte de celle pour laquelle les données ont été initialement collectées ;

[41] Article 104 LIL.

[42] A noter qu'il ne s'agit pas de citer l'ensemble des destinataires visés dans la partie « destinataires » du document, les destinataires étant définis par chaque organisme d'assurance.

✎ les conditions de transferts de données vers un pays tiers ou une organisation internationale en précisant sur quelles dispositions légales a lieu ce transfert et les moyens d'obtenir une copie ou l'endroit où elles ont été mises à disposition.

En outre, uniquement lorsque les données n'ont pas été collectées auprès de la personne concernée :

✎ Les catégories de données traitées ;

✎ la source[43] d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public.

Les informations complémentaires spécifiques à la fraude

En matière de lutte contre la fraude, il existe 2 niveaux d'information :

Premier niveau :
Information générale des personnes concernées sur l'existence d'un dispositif de lutte contre la fraude pouvant conduire à l'inscription sur une liste des personnes présentant un risque de fraude. Il existe des modalités d'information distinctes en fonction des personnes visées :

✎ Pour la fraude interne :

• les salariés du responsable de traitement sont informés individuellement dans le règlement intérieur ou dans tout autre support de communication échangé lors de l'exécution du contrat de travail qu'il existe un traitement visant la lutte contre la fraude interne et externe au sein de l'organisme ;

• les prestataires, les mandataires, les intermédiaires, les administrateurs, les mandataires sociaux ou les élus des organismes sont informés dans les documents contractuels ou tout autre support de communication adressés par le responsable de traitement.

✎ Pour la fraude externe :

• les prestataires, les agents généraux, les intermédiaires sont informés dans les documents contractuels ou tout autre support de communication adressés par le responsable de traitement ;

• les personnes concernées sont informées de l'existence du traitement de lutte contre la fraude, au moyen des documents qui leur sont communiqués au moment de la souscription du contrat, ou de tout autre support de communication échangé lors de l'exécution du contrat. Cette information vise également la mise en œuvre du dispositif mutualisé des données des contrats et des sinistres déclarés auprès des assureurs, mis en œuvre par l'ALFA pour les contrats d'assurance automobile.

Second niveau :
En cas de détection d'une anomalie, d'une incohérence ou d'un signalement susceptible de relever d'une fraude, le responsable de traitement a la possibilité d'inscrire une personne sur une « liste de personnes présentant un risque de fraude ». La personne concernée, susceptible d'être inscrite sur cette liste, peut être un assuré, un prestataire, un professionnel de santé etc. (Il s'agit des personnes concernées par la mise en œuvre du traitement de lutte contre la fraude interne et externe).

Au cours de la période d'investigation, la personne concernée pourra être contactée, selon le type de fraude suspectée (assuré, partenaire, salarié…), pour apporter des éléments complémentaires. Au terme des investigations, en cas de décision prise produisant des effets juridiques (ex. : refus de prise en charge, avertissement au salarié, rupture de contrat), une information écrite et individuelle est adressée précisant les mesures prises par l'assureur et lui donnant la possibilité de présenter ses observations, sans préjudice des dispositions légales applicables.

[43] Ex : organisme public ou privé

8

Droits des personnes concernées

Le responsable de traitement met en œuvre les droits de la personne concernée gratuitement.

Le responsable de traitement doit dans les meilleurs délais et au plus tard dans un délai d'un mois à compter de la réception de la demande :

- répondre à la demande d'exercice des droits de la personne concernée afin d'y donner suite ou non. Dans le cas où le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel ;
- le cas échéant, indiquer que le délai de réponse sera prolongé de deux mois compte tenu de la complexité et du nombre de demandes.

Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

Le responsable de traitement peut refuser de faire droit à la demande de la personne concernée notamment dans les cas suivants :

- lorsqu'il n'est pas en mesure d'identifier la personne en faisant la demande ;
- lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif ou de la difficulté technique à structurer les données. Dans cette hypothèse il peut également exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées.

Droit d'accès, de rectification, d'opposition[44]

Le droit d'accès permet à la personne concernée de demander au responsable d'un traitement s'il détient des données personnelles sur elle et, dans l'affirmative, de lui demander qu'on les lui communique.

Le droit de rectification permet à la personne concernée de demander la rectification des données personnelles la concernant lorsqu'elles sont inexactes. Il permet également à la personne concernée de demander à ce que ses données personnelles soient complétées si elles sont incomplètes, dans la mesure où cela est pertinent au regard de la finalité du traitement en cause.

Le responsable de traitement notifie la rectification à chaque destinataire auquel les données à caractère personnel ont été communiquées à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

[44] Pour plus d'informations : https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles

Le droit d'opposition permet à la personne concernée de s'opposer au traitement lorsque ce traitement est fondé sur l'intérêt légitime du responsable de traitement. Sauf exception, la personne concernée doit invoquer des raisons tenant à sa situation particulière. Ce droit s'exerce sous réserve de justifier d'un motif légitime de la personne concernée tenant à sa situation particulière. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. En matière de prospection commerciale, ce droit d'opposition peut s'exercer sans avoir à justifier d'un motif légitime.

Droit à la limitation du traitement

Le droit à la limitation du traitement est possible dans quatre cas :

- la personne concernée conteste l'exactitude des données ;
- le traitement est illicite et la personne s'oppose à l'effacement des données et exige à la place la limitation de leur utilisation ;
- le responsable de traitement n'a plus besoin des données pour le traitement mais elles sont encore nécessaires à la personne concernée en cas de constatation, exercice ou défense des droits en justice ;
- la personne s'est opposée au traitement pour des motifs légitimes.

La limitation entraine le gel temporaire du traitement des données qui ne peuvent plus faire l'objet que d'une conservation sauf si :

- la personne concernée donne son consentement à une autre forme de traitement ;
- leur traitement est nécessaire à « *la constatation, l'exercice ou la défense de droits en justice (…), la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre* ».

Le responsable de traitement doit informer la personne concernée avant la levée de cette mesure.
Le responsable de traitement notifie la limitation du traitement effectué à chaque destinataire auquel les données à caractère personnel ont été communiquées à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

Droit à la portabilité des données

Le droit à la portabilité permet à la personne concernée de recevoir ou d'obtenir que soient transmises à un autre responsable de traitement (si cela est techniquement possible) les données personnelles la concernant et remplissant les conditions cumulatives suivantes :

- les données qu'elle a personnellement fournies (ex : nom, adresse, âge, déclaration du sinistre…). Sont exclues, les données anonymisées et les données déduites ou dérivées (ex : analyse des données brutes d'un boitier connecté, résultat d'une appréciation relative à la santé d'un utilisateur en assurance emprunteur) ;
- les données dont le traitement a pour base juridique, soit l'exécution d'un contrat auquel la personne concernée est partie ou l'exécution de mesures précontractuelles prises à la demande des personnes, soit le consentement de la personne concernée ;
- les données sont traitées de manière automatisée (les fichiers papiers ne sont pas concernés).

Données portables

À titre indicatif, les données portables sont les suivantes :

- Les données d'identification relatives à l'état civil, à la nationalité et aux coordonnées…
- Les données relatives à la situation familiale
- Les données relatives à la situation économique, patrimoniale et financière
- Les données relatives à la situation professionnelle
- Les données relatives aux demandes de versements, aux avances, aux opérations de rachat, aux arbitrages.
- Les données nécessaires à l'appréciation du risque
- Les déclarations de sinistre
- Les données fournies par la personne concernée nécessaires à la détermination ou à l'évaluation des préjudices et des prestations
- Les données brutes issues des objets connectés

Données non portables (car données déduites ou dérivées)

À titre indicatif, les données non portables sont les suivantes :

- Les statistiques
- Le profil élaboré au moyen notamment des données directement fournies ou de celles issues des objets connectés
- Les données nécessaires à la passation, la

gestion et l'exécution du contrat (générées notamment du fait de l'exécution du contrat) : le numéro d'identification du client, de l'assuré, du contrat, le montant des primes, des cotisations et accessoires, des commissions, des taxes, des créances en cours, les références de l'apporteur, des coassureurs et des réassureurs, la durée du contrat, les garanties, les montants, les exclusions, , le détail de l'opération relative au produit ou service souscrit, les relevés d'impayés.

- Les données relatives à l'identification des personnes intervenantes au contrat : 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 données nécessaires à la gestion des sinistres et des prestations : le numéro du dossier sinistre, les rapports d'expertise, les rapports d'enquête, les données transmises par les régimes obligatoires de sécurité sociale, les organismes de retraites.

Données non portables (car données traitées sur le fondement de l'intérêt légitime, d'une obligation légale)

A titre indicatif, les données non portables sont suivantes :

- Les données relatives à la fraude (anomalies, incohérences et signalements, investigations etc.)
- Les données de la LCB/FT
- Les données relatives au prélèvement à la source ou relatives à d'autres obligations déclaratives (URSSAF…)
- Les données relatives aux personnes dans le cadre de la prospection commerciale (hors prospection par voie électronique) si l'intérêt légitime peut être démontré.

Droit d'obtenir une intervention humaine

Les responsables de traitement dans le secteur de l'assurance peuvent avoir recours à des décisions individuelles automatisées au sens de l'article 22 du RGPD, c'est-à-dire des décisions produisant des effets juridiques concernant la personne concernée ou l'affectant de manière significative de façon similaire (voir supra).

Le recours à ce type de décisions est possible dans la mesure où elles sont nécessaires à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable de traitement ou sont fondées sur le consentement explicite de la personne concernée. De telles décisions ne peuvent être fondées sur des catégories particulières de données (ex : données de santé) que si l'assuré a donné son consentement explicite ou lorsque le traitement est nécessaire pour des motifs d'intérêt public.

Lorsque le responsable de traitement a recours à ce type de décision individuelle automatisée, la personne concernée a le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

Droit de retirer son consentement

La personne concernée dispose, lorsque la base légale du traitement est le consentement, d'un droit de retrait de son consentement.

Ce retrait ne compromet pas la licéité du traitement effectué avant le retrait.

Il fera cesser le traitement mais n'ouvre pas un droit à résiliation du contrat d'assurance.

Par exemple, la personne concernée peut retirer son consentement à la réception d'offres commerciales par voie électronique.

Droit à l'effacement

Le droit à l'effacement oblige le responsable de traitement à effacer dans les meilleurs délais toutes les données (celles d'origine et celles enrichies) de la personne concernée :

❶ lorsqu'elles ne sont plus nécessaires au traitement

❷ ou lorsque le traitement cesse du fait :

- du retrait du consentement et qu'il n'existe pas d'autre fondement juridique au traitement (par ex. période de conservation) ;
- du droit d'opposition et qu'il n'existe pas de motif légitime impérieux pour le traitement ;
- de l'illicéité du traitement ;

❸ ou afin de respecter une obligation légale.

Le responsable de traitement notifie l'effacement à chaque destinataire auquel les données à caractère personnel (cela vise toutes les copies ou reproductions) ont été communiquées à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

Voies de recours de la personne concernée

La personne concernée dispose en matière de voies de recours d'un droit :

- d'introduire une réclamation auprès d'une autorité de contrôle de protection des données (ex : CNIL en France) dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise ;
- à un recours juridictionnel effectif contre une autorité de contrôle de protection des données ;
- à un recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement ou devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle ;
- de se faire représenter y compris dans le cadre d'une action de groupe ;
- à réparation.

Autres droits

La personne concernée a la possibilité de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès dans les conditions de l'article 85 de la loi informatique et libertés du 6 janvier 1978.

9

Destinataires

Le destinataire est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

Destinataires communs à tous les traitements

Peuvent avoir accès aux données à caractère personnel dans les limites de leurs attributions respectives en fonction des traitements concernés:

dans le cadre des missions habituelles qui leur sont assignées et dont ils doivent répondre:

- les personnels chargés de la gestion commerciale clients/prospects ou de la passation, la gestion et l'exécution des contrats;
- les délégataires de gestion, les intermédiaires d'assurance, les partenaires;
- les prestataires;
- les co-responsables de traitement
- 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;
- les responsables de traitement chargés dans le cadre d'un contrat de partenariat de gérer les contrats d'assurance du responsable de traitement, y compris dans le cadre d'un réseau de soins;
- s'il y a lieu les assureurs des personnes impliquées ou offrant des prestations complémentaires;
- s'il y a lieu les coassureurs et réassureurs, les intermédiaires de réassurance 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 responsables de traitement offrent des garanties complémentaires à celles des régimes sociaux;
- les organismes et associations pratiquant la prévention, l'action sociale ou la gestion de réalisations sanitaires et sociales.
- les services chargés du contrôle (services chargés des procédures internes du contrôle...)

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 ou leurs ayants droit, ainsi que leurs représentants ; les témoins, les tiers intéressés à l'exécution du contrat.

en qualité de personnes bénéficiant d'un droit de communication :

- 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.

Destinataires spécifiques à certains traitements

Dans le cadre de la prospection commerciale

Peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel :

- les personnes chargées du service marketing, du service commercial, des services chargés de traiter la relation client, les réclamations, et la prospection, des services administratifs, des services logistiques et informatiques ainsi que leurs responsables hiérarchiques ;
- les services chargés du contrôle (commissaire aux comptes, services chargés des procédures internes du contrôle…) ;
- les sous-traitants.

Peuvent être destinataires des données :

- les partenaires et sociétés extérieures (sociétés avec lesquelles l'entreprise entretient des relations commerciales régulières), les entités du groupe de sociétés ;
- les auxiliaires de justices, les officiers ministériels et organismes publics habilités à les recevoir, les arbitres, les médiateurs.

Dans le cadre de la consultation du RNIPP par l'intermédiaire de l'AGIRA aux fins de recherche des assurés et bénéficiaires de contrats d'assurance vie décédés

Les personnes habilitées à recevoir communication de ces données sont :

au sein de l'AGIRA : les gestionnaires habituels chargés de l'exploitation des fichiers.

au sein des responsables de traitement : les gestionnaires habilités.

Dans le cadre de la lutte contre la fraude

Aux fins de lutte contre la fraude interne :

- les personnes habilitées de la direction des ressources humaines pour des requêtes ponctuelles et individuelles réalisés dans le cadre d'enquêtes internes consécutives à la détection d'une fraude,
- le conseil de discipline saisi en cas de fraude ;
- les représentants du personnel dans le cadre de l'accompagnement d'un salarié mis en cause pour fraude.

Aux fins de lutte contre la fraude interne et externe :

- les personnels en relation avec la clientèle et les gestionnaires de contrats et de sinistres ;
- les autres entités d'un même groupe dès lors qu'elles sont concernées par la fraude ou interviennent dans la gestion des dossiers ou de maîtrise du risque de fraude ;
- les personnels habilités en charge de la lutte contre la fraude, de la lutte anti-blanchiment et du contrôle interne, les inspecteurs, enquêteurs, experts, et auditeurs ;
- le personnel habilité de la direction générale, la direction juridique ou du service du contentieux pour la gestion des contentieux ;
- le personnel habilité des sous-traitants.

Dès lors qu'ils sont directement concernés par une suspicion de fraude, peuvent être destinataires des données relatives à cette fraude, les personnels habilités :

- par les autres responsables de traitement intervenant dans le cadre du dossier présentant une fraude ;
- des organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les responsables de traitement offrent des garanties complémentaires à celles des régimes sociaux ;
- des organismes professionnels intervenant dans le cadre de dossiers présentant un risque de fraude pour les seules données concernées par ce dossier ;
- les auxiliaires de justice et officiers ministériels ;
- l'autorité judiciaire, médiateur, arbitre saisis d'un litige ;

- les organismes tiers autorisés par une disposition légale à obtenir la communication de données à caractère personnel relatives à des précontentieux, contentieux ou condamnations ;
- s'il y a lieu les victimes de fraudes ou leurs représentants.

La communication de ces données ne donne pas lieu à la création d'un fichier concernant les données relatives aux fraudes et mutualisé entre les destinataires.

Le dispositif ALFA mutualise pour l'assurance automobile des données des contrats d'assurance et des sinistres pour identifier des alertes impliquant plusieurs assureurs.

Dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme et du respect des sanctions économiques et financières internationales

Parmi les responsables de traitement :

- les personnes en relation avec la clientèle et les gestionnaires de contrats et de sinistres pour les clients dont ils ont la charge à l'exception des informations relatives aux déclarations de soupçon.
- les personnes habilitées à prendre la décision de nouer ou de maintenir une relation d'affaires avec une personne politiquement exposée (PPE).
- les personnels habilités du (ou des) service(s) chargé(s) de la lutte contre le blanchiment, notamment ceux ayant la qualité de correspondant ou de déclarant Tracfin, au sein de l'organisme responsable du traitement.
- les autres entités d'un même groupe dès lors qu'elles sont concernées par la lutte contre le blanchiment et le respect des sanctions économiques et financières internationales ou qu'elles interviennent dans la gestion des dossiers ou de maîtrise de ces risques
- lorsque l'organisme financier fait partie d'un groupe au sens de l'article L.511-20, III du CMF ou de l'article L334-2 du Code des assurances, les services de lutte contre le blanchiment des entreprises du même groupe dont le siège social est situé dans un État membre de la Communauté européenne, dans un État partie à l'accord sur l'Espace économique européen ou dans un État dont les autorités ont conclu avec l'Autorité de contrôle prudentiel une convention bilatérale en application des articles L 632-7, L 632-13et L 632-16 du CMF, sous réserve que cet État ait été reconnu par une décision de la Commission européenne comme assurant un niveau de protection adéquat,

Parmi les autorités compétentes :

- la cellule de renseignement financier Tracfin du ministère de l'économie, des finances et de l'industrie,
- les autorités de contrôle compétentes au sens de l'article L561-36 du CMF,
- pour les données relatives aux personnes qui font l'objet d'une mesure de gel des avoirs, la Direction Générale du Trésor,
- les autorités de contrôle compétentes des autres états membres de la Communauté européenne, des états parties à l'accord sur l'Espace économique européen et des états où sont applicables les accords conclus avec l'Autorité de Contrôle Prudentiel et de Résolution ou l'Autorité des Marchés Financiers en application des dispositions prévues aux articles L632-7, L632-13 et L 632-16 du CMF.

Parmi les autres organismes financiers :

- les personnes visées au II de l'article L 561-7 du CMF
- les personnels habilités des autres organismes visés à l'article L 561-20 du CMF, les compagnies financières et les compagnies financières holding mixtes, lorsqu'ils appartiennent à un même groupe tel que défini au III de l'article L 511-20 du CMF ou à l'article L 334-2 du Code des assurances, en ce qui concerne l'existence et le contenu de la déclaration de soupçon,
- dans le respect des conditions posées à l'article L 561-21 du CMF, les autres organismes qui interviennent pour le même client dans la même transaction, en ce qui concerne l'existence et le contenu de la déclaration de soupçon.

10

Durées de conservation

Les données personnelles ne peuvent être conservées de façon indéfinie : une durée de conservation doit donc être déterminée en fonction de la finalité ayant conduit à la collecte de ces données.

Les durées de conservation correspondent aux délais pendant lesquels les responsables de traitement peuvent être amenés à traiter la donnée collectée.

Les durées indiquées ci-après correspondent par conséquent aux durées pendant lesquelles les données doivent être conservées par les responsables de traitement. **Elles peuvent faire l'objet d'un archivage.**

En l'absence de conclusion du contrat d'assurance

Gestion de la prospection

Les données relatives à un prospect non-client sont conservées pendant un délai de **3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect**[45] (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel renvoyant vers le produit promu ; en revanche, l'ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect).

Au terme de ce délai, le responsable de traitement peut reprendre contact avec la personne concernée pour lui demander si elle souhaite toujours recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées.

Données de santé

Les données de santé sont conservées pendant une durée maximale de **5 ans à compter de leur collecte ou du dernier contact émanant du prospect (2 ans en base active et 3 ans en archivage intermédiaire)**[46].

[45] Référentiel CNIL Gestion commerciale

[46] Ancienne norme simplifiée n° 16

Cette durée se justifie par le fait que le responsable de traitement doit pouvoir répondre aux demandes formulées par un assuré en cas de contestation à la suite d'un refus ou mise en cause de sa responsabilité (par exemple pour une demande dans le cadre d'une assurance emprunteur) ou en cas de demandes de médiation.

Statistiques des mesures d'audience

Les recommandations de la CNIL « cookies et autres traceurs » adoptées le 17 septembre 2020 (Délibération n° 2020-092), établissent les règles relatives à la durée de conservation des informations stockées dans le terminal des utilisateurs ou de tout autre élément utilisé pour les identifier et les tracer.

Lorsqu'un contrat d'assurance est conclu

La durée de conservation tient compte de deux paramètres :

- **la durée de l'engagement** (la prestation sera versée jusqu'à la date x , les réclamations des tiers lésés sont garanties pendant X ans après la fin du contrat)
- **le délai de prescription** (c'est-à-dire le délai pendant lequel le bénéficiaire du droit peut agir pour demander à en bénéficier, dont le point de départ varie en fonction de l'action – voir b) ci-dessous).

Enfin, d'une façon générale, sur le plan comptable, le responsable de traitement doit être en mesure de présenter, pendant une durée de 10 ans, tout document nécessaire pour prouver le paiement et le montant du paiement[47].

Les durées mentionnées ci-après, ne constituent pas un recensement exhaustif des durées de conservation nécessaires et indiquent des durées théoriques que les entreprises adaptent en considération de leurs traitements spécifiques.

❶ Durées de conservation légales ou réglementaires applicables aux sociétés d'assurance

Doivent être pris en compte :

- les délais de conservation des documents sur lesquels peuvent s'exercer les droits de communication, d'enquête et de contrôle des autorités fiscales : **6 ans** (dans certains cas **10 ans**) **à compter de la date de la dernière opération** mentionnée sur les livres ou registres ou de la date à laquelle les documents ou pièces ont été établis (article L.102 B du Livre des procédures fiscales) ;
- les délais de conservation des documents et informations relatifs au client et aux opérations faites par ceux-ci dans le cadre de la lutte contre le **blanchiment et le financement du terrorisme : 5 ans à compter de la clôture de leurs comptes ou de la cessation de la relation ou à compter de l'exécution des opérations.** (article L. 561-12 du Code monétaire et financier).
- les délais de conservation de l'écrit qui constate les contrats conclus par voie électronique et portant sur une somme supérieure à 120€ : **10 ans à compter de la conclusion du contrat** (L. 213-1 du Code de la consommation).

❷ Durées de conservation et règles de prescription propres aux contrats d'assurance

Les assureurs qui couvrent la responsabilité civile sont susceptibles d'indemniser la victime d'un dommage aussi longtemps que celle-ci peut agir en justice pour faire valoir ses droits.

Ainsi, les délais de prescription prévus par le Code civil et le Code de procédure pénale[48] et les délais de prescription spécifiques prévus par le Code des assurances doivent être pris en compte.

Les paragraphes ci-après, donnent quelques exemples de durées de conservation applicables aux contrats d'assurance dommage, d'assurance de personnes. Des particularités propres à certains types de contrats doivent être prises en compte, comme par exemple, l'assurance construction[49], ou l'assurance de risques situés dans d'autres pays et soumis à une législation locale en matière de prescription.

[47] Article A 343-4-1 du Code des assurances: Les informations relatives à ces documents doivent être à tout moment d'un accès facile et comporter au moins les éléments suivants : - soit numéro du contrat ou de l'avenant, soit numéro de l'assuré ou du sociétaire avec tous les contrats ou avenants le concernant ; - date de souscription, durée du contrat ; - nom du souscripteur, de l'assuré ; - éventuellement nom ou code de l'intermédiaire ; - date et heure de la prise d'effet stipulée au contrat ; - date et motif de la sortie éventuelle ; - monnaie dans laquelle le contrat est libellé ; - type de garantie par référence aux catégories d'assurance définies à l'article A. 344-2 ; - montant des limites de garantie, du capital ou de la rente assurée.

[48] Notamment : Actions personnelles ou mobilière (article 2224 du Code civil), Actions en responsabilité nées en raison d'un dommage corporel (article 2226 du Code civil), action réelle immobilière (article 2227 du Code Civil), action civile devant les juridictions pénales (article 10 du Code de procédure pénale)

[49] La surveillance prudentielle d'un exercice sur une durée de 15 ans.

Garanties RC

❶ En cas de sinistre matériel, les données sont conservées le temps de gestion du sinistre et 10 ans à compter de sa clôture[50].

❷ En cas de sinistre corporel, les données sont conservées le temps de gestion du sinistre et 50 ans à compter de sa clôture[51].

❸ En cas d'absence de sinistre :

• **Pour les garanties RC en base « réclamation » :** Selon la durée de la garantie subséquente, les données rattachées au contrat peuvent être conservées **12 ans à compter de la résiliation du contrat**[52].

• **Pour les garanties RC en base « fait dommageable » :** Les données rattachées au contrat peuvent être conservées **22 ans à compter de la résiliation du contrat** (20 ans selon la prescription prévue par le Code civil pour l'action de la victime contre le responsable[53] + 2 ans prescription du Code des assurances pour l'assuré contre son assureur[54]).

Garanties dommages (hors cas particuliers)

Les données sont conservées **10 ans à compter de la clôture du sinistre ou de la résiliation du contrat**[55].

Assurance vie – En cas de vie

Les données sont conservées **30 ans à compter du rachat total ou de la résiliation**[56].

Assurance vie – En cas de décès

Les données sont conservées **30 ans à compter du décès**[57].

Assurance Emprunteur

Les données sont conservées **10 ans à compter de la fin des engagements contractuels**[58].

Assurance complémentaire - Prévoyance

Les données sont conservées **10 ans après le paiement de la prestation ou de la résiliation du contrat**[59].

Traitements LAF

Étape n°1 Qualification de l'alerte : à compter de l'émission de l'alerte, les organismes d'assurance disposent d'un délai de 6 mois pour qualifier les alertes. Il est recommandé que toute alerte « non pertinente » ou n'ayant reçu aucune qualification, **soit supprimée immédiatement** à l'issue d'un **délai de quelques mois (6 mois par exemple).**

Étape n°2 Alerte qualifiée : lorsque l'alerte est « pertinente » les données sont conservées pour une **durée maximale de 5 ans à compter de la clôture du dossier de fraude.** En cas de procédure judicaire, elles sont conservées jusqu'au terme de la procédure. Elles sont ensuite archivées.

S'agissant de la possibilité d'inscription dans le fichier des personnes présentant un risque de fraude, il est recommandé de conserver les données pendant une **durée de 5 ans à compter de la date d'inscription**[60].

[50] Article L123-22 du Code de commerce

[51] Pour tenir compte du droit de la victime de rouvrir son dossier sinistre en cas d'aggravation de ses dommages corporels conformément à l'article 2226 du code civil.

[52] Ce délai prend en compte d'une part un délai 10 ans de prescription liée aux engagements comptables et d'autre part le délai de 2 ans de prescription de l'action contre l'assureur de responsabilité qui s'ajoute au délai de prescription de l'action de la victime contre le responsable assuré.

[53] Article 2224 et 2232 du Code civil

[54] Article L.114-1 du Code des assurances

[55] Notamment en raison des engagements comptables

[56] Article L. 114-1 du Code des assurances : En effet, outre le délai de 2 ans prévu par l'article L.114-1 applicable aux actions de l'assuré, et du délai de 10 ans prévu par l'article L.123-22 du code de commerce en matière comptable, des tiers peuvent exercer des actions en affirmant que le paiement n'a pas eu lieu et qu'ils bénéficient du délai de prescription de 30 ans. L'assureur doit alors prouver qu'il a effectué le paiement de la prestation. Enfin, l'exemple des spoliations intervenus pendant la 2nde guerre mondiale a montré l'utilité pour les personnes concernées que l'assureur conserve les informations relatives à l'assurance vie pendant une durée suffisamment longue

[57] Pour les mêmes raisons que celles exposées au renvoi précédent

[58] Article L123-22 du Code de commerce

[59] En raison des engagements comptables

[60] Le délai d'obligation de conservation des informations relatives aux soupçons de blanchiment est de 5 ans. Or les soupçons de blanchiment sont alimentés par des cas de fraude qui concernent des faits susceptibles de relever de qualifications pénales de délits en cas de poursuite pénale

11

Mesures de sécurité

Le responsable du traitement prend les mesures appropriées afin de garantir un niveau de sécurité adapté aux risques présentés par les traitements mis en œuvre. Ainsi, il prend toutes précautions utiles, notamment techniques et organisationnelles, pour préserver la sécurité, l'intégrité, la disponibilité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

Le responsable de traitement définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille du responsable de traitement ou de ses coresponsables de traitement ou de ses sous-traitants. Cette politique devra décrire les objectifs de sécurité et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.

Une gestion des habilitations permettant de limiter l'accès aux données aux seules personnes dument habilitées et autorisées à les connaitre en fonction de leur profil est nécessaire.

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...).

En cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, le responsable du traitement doit la notifier, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à l'autorité de protection des données compétente.

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel aux personnes concernées dans les meilleurs délais, à moins que cette communication ne soit pas nécessaire pour l'une des conditions prévues par le RGPD.

Mesures de sécurité spécifiques au traitement des données médicales

Rappelons que les données médicales sont couvertes par le secret professionnel ce qui implique l'intervention de professionnels de santé ou de personnes spécifiques soumises au secret professionnel agissant sous leur autorité et les traitements des données collectées sont alors réalisés dans le respect du code de bonne conduite annexé à la convention AERAS.

Juillet 2021 / **Conception graphique :** Vanessa Vansteelandt