ASSOCIATION DES PROFESSIONNELS DE LA RÉASSURANCE EN FRANCE

Règlement Européen Data Protection

Note pour la Réassurance

1. Introduction

1.1. Objectifs de la note

Cette note est issue d'un travail collaboratif des membres de l'APREF[1] et notamment du Comité Vie et de la Commission Juridique.

Elle ne constitue en aucun cas un code de bonne conduite au sens de la réglementation en vigueur, ou un code de conduite au sens du Règlement Européen.

Cette note a pour objet d'aider à la mise en place du Règlement Européen au vu de la particularité des activités de réassurance.

1.2. Executive Summary

L'adoption du Règlement Européen sur la protection des données personnelles le 24 mai 2016, pour une application à compter du 25 mai 2018, marque un tournant majeur dans la réglementation des données personnelles.
Le règlement renforce les droits des personnes physiques et leur donne plus de contrôle sur leurs données personnelles. Il simplifie les formalités pour les entreprises et leur offre un cadre juridique unifié.

Ainsi, en complément du droit à l'information, du droit d'opposition et de rectification de ses données personnelles, la personne physique se voit doter avec le règlement des nouveaux droits suivants :

- Le droit à l'oubli permettant aux personnes concernées de demander l'effacement de ses données personnelles ;
- Le droit à la portabilité offrant la possibilité de transférer ses données personnelles à un tiers.

Au niveau des entreprises, le Règlement Européen renforce les obligations quant aux traitements de ces données à caractère personnel. En effet, même si le nouveau Règlement Européen allège les charges administratives pesant sur les responsables de traitement avec la disparition de la déclaration à la CNIL, en contrepartie les responsables de traitement doivent respecter un certain nombre de grands principes de conformité énoncés dans le règlement :

- Le **principe d'accountability** : le responsable de traitement doit pouvoir apporter la preuve du respect du règlement ;
- Le **Privacy by default** : avec la mise en œuvre de mesures techniques et organisationnelles limitant les traitements aux seules données personnelles nécessaires à la finalité ;
- Le **Privacy by design** : avec la mise en mise en œuvre de mesures techniques et organisationnelles assurant une protection efficace des données dès la conception ;

[1] APREF : Association des Professionnels de la Réassurance en France

- La tenue d'un **registre des traitements** des données par le responsable de traitement ;
- La formalisation **d'études d'impact** pour les traitements comportant un risque élevé pour les droits et libertés ;
- La sécurité des données grâce notamment à leur **pseudo-anonymisation** et le contrôle régulier des systèmes.

Par ailleurs, le règlement formalise la fonction du CIL, appelé désormais « délégué à la protection des données » et a 3 missions principales :

- conseiller le responsable de traitement,
- contrôler la conformité des traitements au règlement, et enfin,
- servir d'interlocuteur à l'autorité de contrôle (ces rôles n'étaient pas formalisés dans les précédentes règlementations).

Au global le règlement demande aux entreprises une plus grande transparence vis-à-vis du citoyen quant à l'utilisation de données à caractère personnel, avec l'obligation d'indiquer aux personnes concernées la durée de conservation et les traitements effectués, associé à un devoir d'information en cas de faille de sécurité.

En outre, les associations représentant les catégories professionnelles sont autorisées à concevoir des codes de conduite spécifiques à leurs secteurs d'activités sur l'application du règlement. Ces codes doivent être approuvés par l'autorité de contrôle. La création de certification et de labels de conformité au règlement est également accordée par le règlement. Pour le secteur de l'assurance, un code de conduite est en cours de rédaction par la FFA.

Les autorités de protection nationales (les « CNIL » européennes), peuvent désormais infliger des sanctions allant jusqu'à 4% du chiffre d'affaires mondial ou vingt millions d'euros au lieu du plafond de trois millions d'euros prévu par la loi pour la République numérique (150 000 euros jusqu'en octobre 2016). De plus, elles peuvent prononcer des décisions conjointes, aussi bien pour constater la conformité d'un organisme que pour le sanctionner. Cette harmonisation européenne renforce ainsi la protection des personnes et la sécurité juridique pour les entreprises.

Table des Matières

2. Définitions et cycle de vie

2.1. Définitions (au sens du Règlement Européen)

Les données personnelles :
« *Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.* »[2]

Les données à caractère particulier (ex données sensibles) :
Le vocable de « données sensibles » provient de la précédente réglementation. Dans le nouveau règlement, elles sont identifiées comme catégories particulières de données à caractère personnel.
Il s'agit des données faisant apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle, ou encore, les données biométriques ou relatives à la génétique.
Leur traitement est interdit par principe, cependant, des dérogations existent.[3]

Le responsable du traitement :
« *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; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.* »[4]

Pseudonymisation de la donnée:
« *Traiter les données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».[5]

Anonymisation de la donnée[6] :
Le Règlement Européen ne définit pas explicitement l'anonymisation des données, mais précise que les données anonymes sortent de son champ d'application.
Les conditions à respecter pour rendre anonymes des données sont particulièrement contraignantes, trois critères doivent être remplis :

- L'individualisation : est-il toujours possible d'isoler un individu ?
- La corrélation : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?
- L'inférence : peut-on déduire de l'information sur un individu ?

Ainsi :

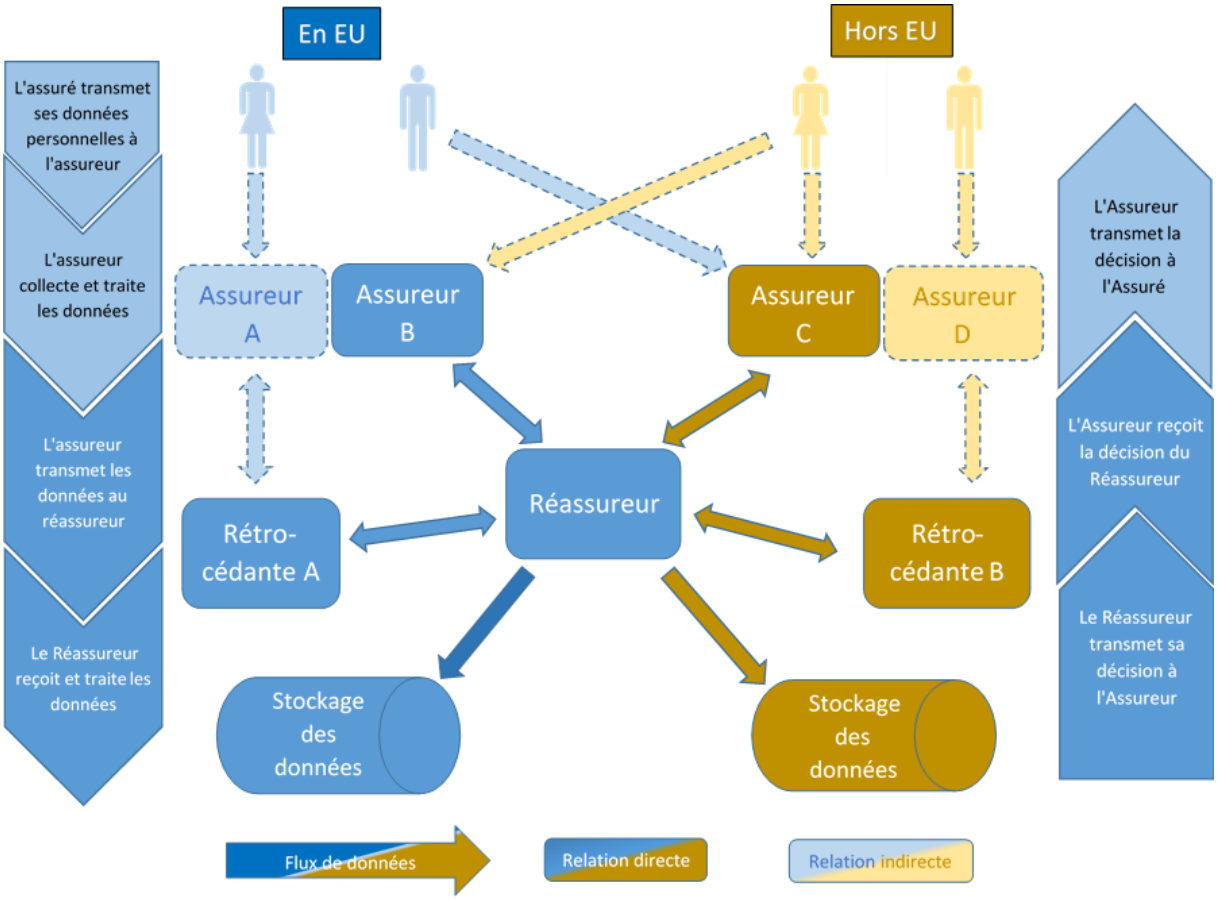
1. un ensemble de données pour lequel il n'est possible ni d'individualiser ni de corréler ni d'inférer est a priori anonyme ;

[2] Article 4 du Règlement (UE) 2016/679
[3] Article 9 du Règlement (UE) 2016/679
[4] Article 4 du Règlement (UE) 2016/679
[5] Article 4 du Règlement (UE) 2016/679
[6] Avis 05/2014 du Groupe de travail « article 29 » sur la protection des données

2. un ensemble de données pour lequel au moins un des trois critères n'est pas respecté ne pourra être considéré comme anonyme qu'à la suite d'une analyse détaillée des risques de ré-identification.

L'anonymisation des données est donc une technique bien particulière ne permettant pas de s'affranchir automatiquement des règles relatives à la protection des données à partir du moment où le nom n'apparait plus.

2.2. Cycle de vie



Remarque : il est rappelé que le réassureur n'est jamais collecteur d'une donnée personnelle d'un assuré/bénéficiaire au titre d'une police d'assurance directe. Il est de la responsabilité de la cédante d'informer l'assuré de la transférabilité de ses données personnelles auprès des réassureurs.

3. Rappel des grands principes légaux actuels

3.1. Les textes fondateurs

3.1.1. L'article 226- 13 du Code pénal

« *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.* »

Cet article du Code Pénal définit non seulement les sanctions auxquelles sont exposées les personnes détentrices du secret professionnel en cas de divulgation, mais également ses modalités de soumission.
Ainsi le secret médical n'est-il qu'une composante du secret professionnel, et le professionnel de santé, qui y est soumis, de par le Code de Déontologie Médicale, ne peut s'en dégager que par effet de la loi.

Par dérogation, le secret professionnel ne peut être partagé que sous certaines conditions cumulatives édictées par l'article 226-2-2 du Code de l'Action Sociale et des Familles : Sans être obligatoire, le partage d'une information à caractère secret n'est autorisé qu'entre deux personnes soumises au secret professionnel, il doit servir un plan d'action visant à soutenir les mineurs et leurs familles, il doit être limité aux seules informations nécessaires, et ne peut se faire sans l'accord préalable des parents sauf intérêt contraire de l'enfant.

Autre dérogation prévue par l'article L1142-12 al 5 de la loi Kouchner du 4 mars 2002, dans le domaine des accidents médicaux, les médecins, missionnés par les Commissions Régionales d'Indemnisation, peuvent mener les opérations d'expertise sans que puisse leur être opposé le secret médical.

3.1.2. Le Code de déontologie médicale

Le Code de Déontologie Médicale, transcrit dans le Code de la Santé Publique dans ses articles R4127-1 à R4127-112, fixe les règles qui s'imposent aux médecins inscrits au tableau de l'Ordre, et les soumet au secret professionnel.

Le secret recouvre toute information portée à leur connaissance dans l'exercice de leur profession. Le terme information doit s'entendre dans son acception la plus large et englobe non seulement ce qui leur a été confié, mais également ce qu'ils ont vu, entendu ou compris.

Le Code de Déontologie précise également le contenu et les modalités de transmission de ces informations (art R4127-45) ; personnels et confidentiels, le dossier médical et la fiche d'observations doivent être actualisés, ils ne sont transmissibles ou accessibles ni aux patients eux-mêmes, ni aux tiers. Ces documents ne peuvent être transmis qu'à un autre médecin participant à la prise en charge ou que le patient souhaite consulter, la transmission n'est possible qu'à sa demande ou avec son consentement, l'accès à son dossier n'est possible que par l'intermédiaire d'un autre médecin (R4127-46).

Le médecin est personnellement responsable de toute indiscrétion relative aux documents médicaux, quels que soient leurs supports, ou toute information qu'il détient (art. R4127-71 à R4127-73).

3.1.3. La directive du 24 octobre 1995 sur la Protection des données

La Directive 95/94 du 24 octobre 1995 est le **premier cadre réglementaire européen en matière de protection des données à caractère personnel.**
En fixant des règles strictes de collecte et traitement, elle a pour objectif de fixer un équilibre entre le droit à la vie privée des personnes et la libre circulation des données. Pour garantir cet équilibre, elle crée dans chaque Etat membre un organisme indépendant en charge du contrôle des activités liées aux traitements des données à caractère personnel.
Son champ d'application se limite aux données traitées par des moyens automatisés (fichiers clients informatiques par exemple) ou contenues, ou destinées à l'être, dans un fichier non automatisé (fichiers papiers).
Le traitement doit s'entendre de la collecte à la destruction des données, chacune de ces étapes constituant un traitement à part entière. Il doit être licite et loyal (à titre d'exemple, les données doivent avoir été collectées avec le consentement de la personne concernée, elles doivent être nécessaires à l'exécution d'un contrat auquel cette personne est partie, au respect d'une obligation légale à laquelle serait soumis le responsable du traitement, ou encore à l'intérêt vital de la personne concernée ; limité aux finalités légitimement, clairement et explicitement déterminées). En dehors des cas listés par la Directive, le traitement de données à caractère personnel est interdit. La conservation des données doit être limitée au temps strictement nécessaire aux finalités pour lesquelles elles ont été collectées.
Certaines catégories de traitements, tels que ceux révélant l'origine raciale ou ethnique, les opinions publiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les traitements de données de santé ou relatives à la vie sexuelle, sont interdites.
La Directive reconnait aux personnes concernées, le droit à l'information (identité du responsable de traitement, finalité du traitement, destinataire des données), le droit d'accès à ces données, et le droit d'opposition.
Le transfert de données à caractère personnel d'un Etat membre vers un pays tiers n'est autorisé que si le niveau de protection est adéquat, même si ce principe comporte quelques exceptions (consentement de la personne concernée, mission d'intérêt public, par exemple).

3.1.4. Convention Belorgey – Convention AERAS

À l'occasion de l'octroi d'un prêt, les établissements de crédit demandent dans la quasi-totalité des cas, la souscription conjointe d'un contrat d'assurance, en garantie du remboursement du prêt. La souscription de ce contrat étant devenue incontournable, l'assurabilité des personnes présentant un risque aggravé de santé est un point déterminant concernant l'accès au crédit des personnes présentant un risque aggravé de santé. Dès 1991, les pouvoirs publics et la FFSA se sont saisis de la question et ont mis en place une convention sur l'assurabilité des personnes séropositives.
Le 19 septembre 2001, les travaux de la commission présidée par le député Jean-Michel Belorgey, ont conduit à la signature d'une convention (dite Belorgey) visant « à améliorer l'accès à l'assurance des personnes présentant un risque aggravé de santé». Cette convention élargit le bénéfice de la convention de 1991 à toutes les personnes présentant un risque aggravé de santé et comporte un volet plus spécifique sur la protection des données des assurés.
Elle institue un code de bonne conduite visant à encadrer la collecte et l'utilisation de données relatives à l'état de santé.
Les principes de ce Code de bonne conduite ont été repris puis développés par la Convention AERAS (s'Assurer et Emprunter avec un Risque Aggravé de Santé) de 2007 révisée en 2011 et 2015.
La protection des données dans le cadre de la convention AERAS se décline dans les procédures de sélection des risques et dans le code de bonne conduite.
1 – Dans les procédures de souscription des contrats emprunteurs: le candidat à l'assurance doit remplir seul le questionnaire de santé quel que soit le support (papier ou informatique) et le transmettre directement au médecin conseil de l'assureur s'il comporte des données de santé. Cette procédure permet de respecter la confidentialité des données échangées avec l'assureur.

2 – Le Code de Bonne Conduite ne s'applique pas seulement à l'assurance des emprunteurs, il a pour périmètre « *toutes assurances intervenant en cas de décès ou d'atteintes corporelles, lors de la déclaration d'un sinistre ou de la demande de prestations* ». Il concilie la confidentialité des données médicales au moment de la collecte et du traitement avec l'activité de l'assureur (appréciation du risque et analyse des sinistres).

Le Code de Bonne Conduite recommande que les sociétés d'assurance soient dotées d'un service médical apte à collecter, analyser et conserver les données de santé.
Dans ce service, les dossiers médicaux sont **placés sous l'autorité d'un médecin**. De plus, afin d'assurer une protection totale des dossiers et des informations de santé, **la confidentialité est organisée physiquement** (le service médical est isolé et doté d'un personnel formé à la confidentialité et au secret professionnel) **et administrativement** (les circuits de communications sont sécurisés). Ces recommandations ont conduit les assureurs à mettre en place les « bulles de confidentialité » qui constituent au sein de l'entreprise d'assurance un lieu étanche dans lequel les données de santé sont traitées et protégées.

3.1.5. Loi du 6/08/2004 – refonte de la loi Informatique et Liberté de 1978

Les premiers principes de protection des données ont été déterminés par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Celle-ci a été modifiée par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel qui transpose la directive européenne du 24 octobre 1995 en droit français.

La loi de 2004 vient consacrer le principe de liberté de circulation des données au sein de l'Union Européenne et restructure la loi de 1978 pour l'adapter aux échanges modernes des données. Elle **crée aussi la fonction de Correspondant Informatique et Libertés** (CIL) qui est garant de la protection des données au sein de l'entreprise dont la présence au sein d'une structure permet d'alléger les procédures.
La loi vient définir la notion **de traitement de données (art.2 al.3), des fichiers automatisés et non automatisés (art.2 al.1).**
Le champ d'application de la loi est **étendu aux données à caractère personnel** (tout élément permettant d'identifier une personne directement ou non), alors que la loi de 1978 se limitait aux données nominatives (art 2 al.2).
Le responsable de traitement (art. 3-I) est défini, il s'agit de la personne physique ou morale qui détermine les finalités et les moyens du traitement.
La loi introduit l'obligation d'information par le responsable de traitement envers la personne faisant l'objet de la collecte des données. Cette dernière dispose d'un droit d'accès, de rectification, d'opposition et de suppression de ses données (art.38 à 40).
Les données de santé sont reconnues comme étant une catégorie de donnée personnelle particulièrement sensible (art.8-1). Par principe, elles sont interdites de collecte, toutefois, la loi en admet la collecte sous réserve de l'accord exprès de l'intéressé (art.8-2).
Le principe de finalité du traitement est posé par l'article 6 de la loi (cf. point B).
Le délai de conservation des données doit être limité à la durée nécessaire pour accomplir la finalité déterminée.
La loi introduit plusieurs niveaux de formalités préalables aux traitements informatisés allant d'un régime allégé à la demande d'autorisation auprès de la CNIL, en passant par la déclaration simplifiée donnant à l'autorité la possibilité pour elle d'établir et de publier des normes pour les catégories de traitements les plus courants. C'est dans ce cadre qu'ont été édictées les **Normes Simplifiées 16 et 56 applicables au secteur de l'assurance (point II A).**
Enfin, la loi vient renforcer les pouvoirs de sanctions (pécuniaires et pénales) et de contrôle de la CNIL.

3.2. 5 grands principes

3.2.1. La finalité du traitement

Le principe de « finalité du traitement » fait partie des principes clés de la loi informatiques et libertés.
Avant toute collecte et utilisation de données personnelles, le responsable de traitement doit précisément annoncer aux personnes concernées ce à quoi elles vont lui servir. Ces objectifs, appelés "finalités", doivent respecter les droits et libertés des individus. Ils limitent la manière dont le responsable pourra utiliser ou réutiliser ces données dans le futur.
Ainsi selon l'article 6-2 I&L :
« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités … »
Deux obligations sont donc mises en avant :
- La réalisation d'une collecte pour des finalités déterminées, explicites et légitimes, ce qui contraint le responsable du traitement à formaliser précisément la finalité pour laquelle un traitement va être réalisé.
- Le principe de « finalité du traitement » implique de ne pas détourner le traitement des finalités initiales.

Une exception est toutefois prévue pour les traitements réalisés à des fins statistiques, historiques ou scientifiques à condition que le traitement soit réalisé dans le respect des autres dispositions légales et qu'il ne soit pas utilisé pour prendre des décisions à l'égard des personnes concernées.

3.2.2. La pertinence des données

Le deuxième grand principe de la protection des données à caractère personnel concerne la pertinence des données : « seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées : *c'est le principe de minimisation de la collecte.* Le responsable de traitement ne doit donc pas collecter plus de données que ce dont il a vraiment besoin. Il doit également faire attention au caractère sensible de certaines données. »
Ainsi l'article 6-3 I&L indique : « [les données] sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs » ; l'article 6-4 précise ensuite : « 4° elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ».
Le principe de minimisation est également présent dans le nouveau Règlement Européen à l'article 5 : « les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ».

3.2.3. La sécurité et la confidentialité des données

Par altération de la sécurité des données on entend toute modification de l'intégrité, de la disponibilité, de l'authenticité ou de la confidentialité des données.
La préoccupation de la sécurité des données rejoint largement celle de la confidentialité des données : toute cyber-attaque ou encore toute rupture de sécurité dans la chaîne de création, utilisation, transmission, sauvegarde, archivage ou destruction de données personnelles vient par définition nuire au respect de la confidentialité de ces données.
Le responsable du traitement fait donc face à une obligation de sécurité. Il doit faire prendre toutes les mesures nécessaires pour garantir la sécurité et la confidentialité des données et éviter leur divulgation (sécurisation des postes de travail, gestion des mots de passe, sécurisation de l'informatique mobile, analyse de risques et politique de gestion des incidents, sécurisation des échanges avec d'autres organismes…).

Les données contenues dans les fichiers ne peuvent être consultées que par les services habilités à y accéder à raison de leurs fonctions. S'il est fait appel à un prestataire externe, des garanties contractuelles doivent être envisagées. Les mesures de sécurité doivent être proportionnées à la nature des données et aux risques présentés par le traitement.

Il est à noter qu'au niveau européen, la directive dite NIS du 18/12/2015 est récemment venue renforcer et uniformiser les exigences sur le niveau de la sécurité des réseaux et des systèmes d'information au sein de l'Europe. Elle s'articule autour des objectifs suivants :

- l'adoption d'une stratégie de sécurité officielle par Etat. Ces stratégies définissent en particulier les politiques de prévention de gestion et de réparation des accidents
- la création de réseaux européens d'équipes de gestion d'incidents informatiques
- la mise en place d'un niveau de sécurité élevé et d'un système de notification pour les organismes d'Importance Vitale ainsi que pour les fournisseurs de services digitaux
- la désignation précise, par Etat-membre, d'autorités administratives compétentes et de points de contacts uniques pour la gestion de la sécurité des réseaux et des systèmes d'information.

En France l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a une mission d'autorité nationale en matière de sécurité et de défense des systèmes d'information et joue un rôle central. Pour ce faire, elle déploie un large panel d'actions normatives et pratiques, depuis l'émission de règles et la vérification de leur application, jusqu'à la veille, l'alerte et la réaction rapide face aux cyberattaques.

3.2.4. La durée de conservation

La Norme Simplifiée numéro 16 de la CNIL (NS 16) prévoit en son article 4 les principes relatifs aux durées de conservation des données à caractère personnel.
La NS 16 permet aux responsables de traitement d'effectuer une déclaration simplifiée auprès de la CNIL concernant « les traitements relatifs à la passation, gestion et exécution des contrats mis en œuvre par les organismes d'assurance […] de réassurance […] ».
Ainsi, sous le contrôle du responsable de traitements, la NS 16 prévoit en cas de :
Conclusion d'un contrat d'assurance:

- Conservation des données : le principe est la conservation pendant la durée du contrat d'assurance ;
- Archivage après la durée du contrat : conservation pendant les durées fixées par le Code des Assurances (art L114-1 et L114-2) relatifs à la prescription (2 ans) et du Code Civil (art 2224 à 2227) (5 ans standard ou 10 ans pour l'action en responsabilité relative à un dommage corporel ou à un préjudice écologique).

En l'absence de conclusion d'un contrat d'assurance :

- Pour les données de santé :
  - 2 ans en archive courante (facilement accessible) et,
  - 3 ans en archive intermédiaire (accès limité)
- Pour les données autres que les données de santé :
  - 3 ans à compter de la collecte ou du dernier contact émanant du prospect.

3.2.5. Le respect des droits des personnes

Les droits des personnes se décomposent comme suit :

3.2.5.1. Le droit à l'information (art. 32 de la loi I&L)

Pour être loyale et licite, la collecte directe (ou indirecte) des données doit s'accompagner d'une information claire et précise des personnes concernées sur :

- la finalité du traitement,
- l'identité du responsable du traitement,
- le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse,
- les destinataires des données,
- leurs droits (droit d'opposition, droit d'accès et de rectification),
- le cas échéant, les transferts de données vers des pays hors UE.

Cette information peut être donnée par tout moyen approprié: courriel, contrat, note interne, mentions légales, avis d'échéance…

3.2.5.2. Le droit d'opposition (art. 38 de la loi I&L)

Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf si le traitement répond à une obligation légale (fichiers des impôts, déclarations fiscales et sociales, casier judiciaire, etc…).
Néanmoins, toute personne a le droit de s'opposer, sans frais et sans motif légitime, à l'utilisation de ses données à des fins de prospection commerciale : c'est la consécration du droit à la tranquillité.

3.2.5.3. Le droit d'accès et de rectification (art. 39 et 40 de la loi I&L)

Toute personne peut, directement auprès du responsable des traitements, avoir accès à l'ensemble des informations la concernant, en obtenir la copie et exiger qu'elles soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.
Le délai de réponse est de deux mois après la demande, sauf pour les données médicales (huit jours après la demande).
Les demandes doivent être accompagnées d'un titre d'identité comportant la signature de la personne concernée (besoin d'identification) et ne pas être manifestement abusives notamment par leur nombre, leur caractère répétitif ou systématique.

3.3. Le traitement des données sensibles

3.3.1. L'interdiction de traitement

L'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, exprime ainsi cette interdiction :
« *Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.* »

3.3.2. Les dérogations

Il existe cependant des dérogations à cette interdiction, au nombre de 8 :

- Lorsque la personne concernée a donné son consentement exprès

- Lorsque les traitements sont nécessaires à la sauvegarde de la vie humaine, dans les cas où la personne concernée ne pourrait donner son consentement.
- Lorsque les traitements portent sur des données à caractère personnel rendues publiques par la personne concernée.
- Lorsque les traitements sont nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.
- Lorsque les traitements sont mis en œuvre par une association ou un organisme à but non lucratif, et à caractère religieux, philosophique, politique ou syndical, et ce à condition qu'ils entrent bien dans l'objet de l'association, qu'ils ne concernent que les membres de cette association et que les données ne soient pas communiquées à des tiers.
- Lorsque les traitements sont nécessaires dans le cadre de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et sont mis en œuvre par un membre d'une profession de santé.
- Lorsque les traitements statistiques sont réalisés par l'INSEE ou tout autre service statistique ministériel agréé.
- Lorsque les traitements sont nécessaires à la recherche, aux études et évaluations dans le domaine de la santé.

Outre les 8 cas spécifiques prévus, une dérogation générale existe lorsque les traitements sont justifiés par l'intérêt public.
On peut observer que l'anonymisation n'est pas prévue dans les dérogations automatiques à l'interdiction générale de traiter des données sensibles. Tout au plus le paragraphe III de l'article 8 dispose que la CNIL peut autoriser certaines catégories de traitements, compte tenu de leur finalité, « Si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi… ».
Si le consentement exprès de la personne concernée lève toute interdiction de traiter des données sensibles, il n'en est pas de même des traitements anonymisés qui doivent faire l'objet d'une autorisation préalable de la CNIL, tel que prévu à l'article 25 – I – 1° .
Il en est de même pour les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques.
La question des données sensibles que l'on recentrera plus particulièrement sur le domaine d'intervention des réassureurs, en l'occurrence sur les données relatives à la santé, génère quelques interrogations à partir de quelques exceptions légales :

- En matière d'accidents de la circulation, l'article R 211-37-5° du Code des Assurances (loi du 5 juillet 1985 – dite Badinter) dispose que la victime est tenue, à la demande de l'assureur, de lui donner ses nom et prénoms, date de naissance, son activité professionnelle, le montant de ses revenus, la description des atteintes à sa personne accompagnée d'une copie du certificat médical initial et autres pièces justificatives en cas de consolidation, son numéro d'immatriculation à la sécurité sociale, etc. Cette communication se fait directement à l'assureur, sans nécessairement transiter par le médecin-conseil.
- En matière d'accidents médicaux, le Code de la Santé Publique prévoit des dispositions à peu près identiques.
- Nous pouvons également citer l'exception légale pour le VIH prévue à l'article L 3122-2 du CSP qui dispose « …dans leur demande d'indemnisation, les victimes ou leurs ayants-droit justifient de l'atteinte par le VIH (…). l'office examine si les conditions d'indemnisation sont réunies ; il recherche les circonstances de la contamination sans que puisse lui être opposé le secret professionnel… »

À la lumière de ces exceptions légales, il est possible de s'interroger sur l'articulation des différents textes avec la loi sur la protection des données personnelles.
La jurisprudence est peu abondante dans ce domaine , la victime ayant intérêt à communiquer toutes les pièces nécessaires à son indemnisation ; toutefois, l'on peut relever un arrêt de la cour d'Appel d'Aix en Provence du 5 octobre 1995 qui a validé le renoncement implicite d'une victime à se prévaloir du secret médical dans un cadre indemnitaire.
En dépit des exceptions légales prévues par les textes, le consentement exprès de la personne concernée reste cependant le moyen le plus sûr pour ne pas risquer de contrevenir aux dispositions de la loi de 1978 (modifiée par la loi du 6 août 2004).

4. Le pack conformité Assurance

4.1. Les normes simplifiées

La CNIL et les représentants de la profession Assurance ont rédigé deux normes : la norme 16 sur la passation, la gestion et l'exécution des contrats d'assurance d'une part et la norme 56 d'autre part sur la gestion commerciale des clients et des prospects pour le secteur de l'assurance
Les normes 16 et 56 explicitent en particulier:
- les finalités de traitements applicables en assurance
- les différentes catégories de données traitées par les assureurs
- les règles encadrant la durée de conservation des données
- les restrictions qui s'appliquent aux destinataires susceptibles d'avoir accès aux données
- l'information des personnes (applicable en particulier dans le cadre de l'utilisation d'un site internet)
- Les droits des personnes (notamment les droits d'accès, de rectification et d'opposition)
- les mesures de sécurité informatiques de rigueur
- l'encadrement du transfert des données en dehors de l'UE

Voir Annexe.

4.2. Les Autorisations Uniques

La collecte du NIR et la consultation du RNIPP (AU 31) – voir document en Annexe 2.
La collecte des données d'infractions, de condamnations ou des mesures de sûreté (AU 32)
La lutte contre la fraude (AU 39) – voir document en Annexe 3.

5. Le Règlement Européen

5.1. Un nouvel écosystème

5.1.1. Les sous-traitants

Il s'agit de la personne physique ou morale, de l'autorité publique, ou du service ou d'un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

5.1.2. Les sanctions administratives

Augmentation conséquente, selon la règle enfreinte, du plafond des sanctions : 20 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Ce plafond peut être ramené à 2% du CA mondial ou 10 millions d'euros.

5.1.3. Les sanctions pénales

Les sanctions pénales sont possibles et laissées à l'appréciation de chaque Etat Membre.
Ces sanctions existent actuellement dans la loi I&L et le Code Pénal, et devraient subsister sauf modificationpar le législateur français.

5.1.4. Les autorités de contrôle compétentes

Le texte pose le principe général de l'indépendance des autorités de contrôle nationales et prévoit un renforcement de leurs moyens.
Ainsi, chaque État membre devra veiller à ce que son autorité dispose de ressources humaines, techniques, et financières appropriées.
Les autorités de contrôle se voient reconnaître le pouvoir de mener des enquêtes, d'arrêter des décisions contraignantes et d'infliger des sanctions administratives.

5.1.5. Le guichet unique

Le règlement prévoit de mettre en place un système de « guichet unique », qui permet, lorsque le responsable de traitement est établi dans plusieurs États membres, de retenir la compétence de l'autorité de contrôle de l'État membre où se situe l'établissement principal du responsable de traitement.

5.1.6. Le mécanisme de cohérence

Afin de contribuer à l'application cohérente du règlement dans l'ensemble de l'Union, les autorités de contrôle de chaque pays coopèrent entre elles et, le cas échéant, avec la Commission dans le cadre du mécanisme de contrôle de la cohérence :

- Un comité est créé à l'échelle européenne, composé des chefs de chaque autorité nationale de protection des données.
- Lorsqu'une des autorités nationales s'apprête à prendre une décision concernant certains sujets listés (article 64) produisant des effets en matière de protection des données, le comité doit être saisi pour avis.

5.2. Les principes de traitement des données

5.2.1. Les principes généraux (articles 5 à 11)

Les données à caractère personnel doivent être :

- « traitées de manière licite et loyale »

- « collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités »
- « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées »
- « Exactes et, si nécessaire tenues à jour….. ».
- « conservées sous une forme permettant l'identification des personnes concernées….. »
- « traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. »

5.2.2. La licéité

Tout traitement de données à caractère personnel doit être licite et loyal. Ces 2 caractéristiques sont complétées par le principe de transparence qui exige que toute information et communication soient facilement accessibles et compréhensibles, et formulées dans des termes clairs et simples. Pour être licite un traitement doit être fondé sur le consentement de la personne concernée ou reposer sur un fondement légitime prévu par la loi, entendue au sens large c'est-à-dire le droit de l'UE ou le droit national.

5.2.3. Le consentement

Le Règlement impose au responsable de traitement de recueillir le consentement de la personne concernée pour traiter ses données personnelles dans le cadre de finalités spécifiques, sauf exceptions.
La nécessité du consentement de la personne concernée induit que le responsable de traitement doit être en mesure de prouver que l'intéressé a consenti à l'opération de traitement de façon éclairée.
La déclaration de consentement rédigée préalablement par le responsable de traitement doit être compréhensible, facilement accessible et formulée dans des termes clairs et simples, et sans clause abusive.
Le consentement doit être donné librement, ce qui implique qu'il ne doit pas y avoir de déséquilibre manifeste entre le responsable de traitement et la personne concernée.
Le consentement peut être retiré à tout moment par la personne concernée.

5.3. Les catégories particulières de données à caractère personnel

Le Règlement étend le qualificatif de données à caractère personnel aux :

- Données de localisation
- Identifiants en ligne
- Adresses IP

En ce qui concerne les catégories particulières de traitement prévues à l'article 9, le texte reprend le principe d'interdiction de collecte des données sensibles avec possibilité sous certaines conditions de lever cette interdiction, par exemple en cas de :

- Consentement explicite de la personne concernée.
- Traitement nécessaire pour l'exécution des droits de la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale.

- Traitement portant sur des données rendues publiques par la personne concernée
- Traitement nécessaire à la constatation ou à l'exercice ou à la défense d'un droit en justice
- Traitement nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique.

L'article 8 de la loi Informatique et Libertés visait expressément les données « qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ».
Le Règlement ajoute à la liste des données sensibles de la Loi I&L :

- Les données génétiques et biométriques (article 9 du Règlement Européen)
- Les données issues des condamnations pénales ou relatives à des mesures de sûreté (article 10 du Règlement Européen)

5.4. Les droits des personnes concernées

La section 3 du Règlement est intitulée « rectification et effacement ». Le droit de rectification se définit comme étant la possibilité pour une personne de rectifier les données à caractère personnel la concernant et qui sont inexactes. La Loi I&L consacre déjà ce droit d'accès et de rectification.

L'article 19 du Règlement s'applique aux droits de la personne concernée à la rectification, l'effacement de ses données personnelles et à la limitation de leur traitement. Il oblige le responsable de traitement à notifier à chaque destinataire de ces données, dont ses sous-traitants, l'exercice de ces droits par la personne concernée.

5.4.1. Le droit à l'effacement (droit à l'oubli numérique)

Par principe, l'article 17 du Règlement Européen reconnait aux personnes concernées « le droit d'obtenir du responsable de traitement l'effacement dans les meilleurs délais, des données à caractère personnel les concernant ».
En parallèle, « le responsable de traitement a l'obligation d'effacer [les] données à caractère personnel dans les meilleurs délais », lorsque l'un des six motifs listés par le Règlement s'applique, par exemple, lorsque la collecte n'est plus nécessaire ou que la personne s'oppose au traitement.

Par exception, le droit à l'effacement ne s'applique pas dans la mesure où le traitement est nécessaire pour respecter une obligation légale qui requiert le traitement et également à des fins statistiques conformément à l'article 89. On peut espérer que la réassurance bénéficiera de la dérogation prévue par l'article 89.

On peut comprendre que les fournisseurs de prestations sur internet (tels que Google ou Facebook) seraient particulièrement visés par ce droit à l'oubli numérique.

5.4.2. Le droit de limiter le traitement

L'article 18 du Règlement Européen consacre au bénéfice de la personne concernée le droit d'obtenir du responsable du traitement, la limitation du traitement. Les données personnelles ne sont alors traitées qu'avec le consentement de la personne concernée. Selon cet article, le traitement des données est limité lorsque l'un des éléments suivants s'applique :

a) L'exactitude des données personnelles est contestée par la personne concernée ;
b) Le traitement est illicite et la personne concernée s'oppose à leur effacement et exige la limitation du traitement ;
c) Le responsable du traitement n'a plus besoin des données à caractère personnel mais celles-ci sont encore nécessaires à la personne concernée ;

d) La personne s'est opposée (art. 21) au traitement dans l'attente de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

5.4.3. Le droit à la portabilité

L'article 20 du Règlement prévoit le droit pour la personne concernée de recevoir ses données à caractère personnel de la part du responsable de traitement « dans un format structuré, couramment utilisé et lisible par une machine ». La personne concernée a le droit de les transmettre à un autre prestataire.

Il apparaît que ce droit est instauré au profit des consommateurs, afin de faciliter la concurrence dans plusieurs secteurs de consommation à l'échelle européenne.

La communication des données individuelles par la cédante à son réassureur n'est pas considérée comme un cas de portabilité puisque le transfert a lieu entre la cédante et le réassureur et ne repasse pas par la personne concernée.

5.4.4. Décision individuelle automatisée, y compris le profilage (« Profiling »)

L'article 22 du règlement dispose que la personne concernée a « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ».

Ce principe ne s'applique pas lorsque la décision est nécessaire à la conclusion ou l'exécution d'un contrat entre la personne concernée et le responsable du traitement, lorsqu'elle est autorisée par le droit de l'Union et lorsque la décision est fondée sur le consentement de la personne.

5.5. Responsabilités (Accountability)

5.5.1. La structure de gouvernance

Le Règlement Européen a des conséquences importantes sur la gouvernance des données personnelles au sein des organismes concernés car ils devront s'adapter à un principe de responsabilité accrue.
Concrètement, cela implique, pour le responsable du traitement, de prendre des mesures efficaces et appropriées afin de se conformer au Règlement Européen (concept d'Accountability) et d'apporter la preuve, sur demande de la CNIL, que les mesures nécessaires ont bien été prises.
Il s'agit d'une démarche de renforcement du cadre de la gouvernance d'entreprise où les notions de contrôle interne et de gestion des risques revêtent une place importante.

Ainsi, le responsable de traitement doit mettre en place un processus permanent et dynamique de mise en conformité à la réglementation grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques correspondantes, résumé comme suit :

- concernant les traitements : la tenue d'une documentation (liste des traitements), l'approche Privacy by Design avec une méthodologie associée, l'analyse d'impact pour les traitements présentant des risques ;
- concernant les personnes concernées : des sessions de formation et de sensibilisation du personnel, une procédure de gestion des droits des personnes concernées, une procédure de gestion des violations de données personnelles ;
- concernant le responsable des traitements : une politique de protection des données écrite et contraignante, le respect de guides d'utilisation ou de codes de bonnes pratiques, la désignation éventuelle d'un délégué à la protection des données (doté d'un réseau de relais et d'outils adaptés), un rapport annuel d'incidents et d'amélioration, des

procédures de vérification pour s'assurer de l'efficacité et l'effectivité des mesures (audits internes ou externe).

Le respect de ces mesures passe notamment, pour certains organismes[7], par **la nomination d'un délégué à la protection des données** qui sera le « chef d'orchestre » de la conformité en matière de données à caractère personnel.

Les missions du délégué à la protection des données sont au moins les suivantes (article 39) :
a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du Règlement et conserver une trace documentaire de cette activité;
b) contrôler le respect du Règlement et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;
c) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci;
d) coopérer avec la CNIL;
e) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, et mener des consultations, le cas échéant, sur tout autre sujet.

Les missions du délégué à la protection des données peuvent aussi être les suivantes :
f) vérifier la notification et la communication en cas de violation de données à caractère personnel;
g) veiller à l'application l'application du « Privacy by design » et la réalisation d'études;
h) veiller à la bonne tenue de la « documentation Informatique et Libertés » du responsable de traitements ou du sous-traitant.

De manière générale, le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

5.5.2. Gouvernance : Politiques et Procédures

Organisation et politique (article 24)

Le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au Règlement.
Lorsque cela est proportionné au regard des activités de traitement, ces mesures comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

Codes de conduite (article 40)

Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du Règlement.

[7] *La nomination d'un délégué à la protection des données est obligatoire lorsque: a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle; b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de données sensibles ou de données relatives à des condamnations pénales ou à des infractions (article 37).*

Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du Règlement.

5.6. Le registre détaillé

Chaque responsable du traitement tient un registre des activités de traitement effectuées sous sa responsabilité.
Ce registre comporte toutes les informations suivantes:

a) ***le nom et les coordonnées du responsable du traitement*** *et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;*
b) les ***finalités du traitement****;*
c) une ***description des catégories de personnes concernées*** *et des catégories de données à caractère personnel;*
d) les catégories de ***destinataires***
e) le cas échéant, les ***transferts*** *de données à caractère personnel* ***vers un pays tiers***
f) dans la mesure du possible, les ***délais prévus pour l'effacement*** *des différentes catégories de données;*
g) dans la mesure du possible, une ***description générale des mesures de sécurité techniques et organisationnelles*** *;*

Chaque sous-traitant tient un **registre** de toutes les catégories d'activités de **traitement effectuées pour le compte du** responsable du traitement, comprenant notamment:

a) le ***nom et les coordonnées du ou des sous-traitants****;*
b) les ***catégories de traitements*** *effectués pour le compte de chaque responsable du traitement;*
c) le cas échéant, les ***transferts*** *de données à caractère personnel* ***vers un pays tiers***
d) les ***mesures de sécurité techniques et organisationnelles*** *;*

Les registres détaillés des traitements peuvent être tenus sous forme électronique. Le responsable du traitement ou le sous-traitant met le registre à la disposition de la CNIL sur demande.

Les obligations de tenue d'un registre ne s'appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur des données sensibles, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions (article 5.1).

5.7. Information des personnes concernées

Le responsable du traitement prend des mesures appropriées pour fournir toute information aux personnes concernées d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

Cf annexe 2

5.7.1. Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée

Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes:

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent;

e) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts vers des pays sans protection adéquate, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

En plus des informations visées ci-dessus, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données;

c) le droit d'introduire une réclamation auprès de la CNIL;

d) des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données;

e) l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

5.7.2. Informations à fournir lorsque des données à caractère personnel n'ont pas été collectées auprès de la personne concernée (article 14)

Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement fournit à celle-ci toutes les informations suivantes:

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement;

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) les catégories de données à caractère personnel concernées;

e) le cas échéant, les destinataires ***ou les catégories de destinataires*** *des données à caractère personnel;*

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts vers des pays sans protection adéquate, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

En complément des informations visées ci-dessus, le responsable du traitement fournit à la personne concernée les informations suivantes nécessaires pour garantir un traitement équitable et transparent à son égard:

a) la durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

b) l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données;
c) le droit d'introduire une réclamation auprès de la CNIL;
d) la source 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;
f) l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Le responsable du traitement fournit les informations visées ci-dessus :

a) 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;

b) 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; ou c) 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.

Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente.

5.7.3. Absence d'obligation d'information

L'obligation d'information ne s'applique pas lorsque et dans la mesure où:

a) la personne concernée dispose déjà de ces informations;
b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ou dans la mesure où l'obligation d'information est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles;
c) 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 du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée; ou
d) les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel.

Le cas d) semble pouvoir s'appliquer aux données médicales transmises dans le cadre de la gestion des contrats d'assurance (cf III.1.4).

5.8. Les mesures techniques et organisationnelles

Les mesures techniques et organisationnelles sont les mesures mises en place par le responsable de traitement (article 24) afin de respecter la réglementation et garantir les droits et libertés de la personne concernée.

Ces mesures techniques et organisationnelles doivent s'appliquer et encadrer :

- La pseudonymisation des données (article 4)
- La conservation des données à caractère personnel (article 5)
- La protection des données, à savoir la minimisation des données où seules les données à caractère personnel nécessaires au traitement sont utilisées ; la minimisation concerne également la quantité de données à caractère personnel collectée, leur durée de conservation, leur accessibilité (article 25)
- La sous-traitance : le responsable de traitement ne peut faire appel qu'à des sous-traitants capables de mettre en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement et garantissant la protection des droits de la personne concernée (article 28)
  En outre lorsqu'un sous-traitant fait appel à un autre sous-traitant, les mêmes obligations s'appliquent et le sous-traitant initial demeure pleinement responsable de l'exécution par l'autre sous-traitant (article 28).
- Sécurité du traitement : le responsable du traitement et le sous-traitant doivent garantir un niveau de sécurité adapté au risque (article 32), y compris entre autres, selon les besoins :
  - la pseudonymisation et le chiffrement des données à caractère personnel;
  - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
  - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
  - une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

5.9. La notification des violations de données

Une violation de la sécurité des données, susceptibles d'affecter les droits et les intérêts des personnes concernées, doit être notifiée :

- à l'autorité de contrôle compétente sous 72 heures
- à la personne concernée si le risque est élevé et les données non chiffrées

Toute violation de données déclarées aux autorités compétentes doit :

- décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
- communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
- décrire les conséquences probables de la violation de données à caractère personnel;

- décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Cette communication précise en des termes clairs et simples, la nature de la violation de données à caractère personnel.

5.10. La protection des données dès la conception

- *La protection des données dès la conception (Privacy by Design) et par defaut (Privacy by Default)*
  Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut. Par exemple, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).
  Il s'agit d'une réponse à la multiplication des traitements de données personnelles par des objets et technologies de tous les jours, qui récoltent toujours plus de données personnelles et qui sont toujours plus interconnectés. Il s'agit aussi d'une réponse aux stratégies de collecte et d'utilisation de données personnelles de certaines entreprises, qui tentent de décourager les particulier de protéger au mieux leurs données personnelles en recourant à des procédures longues, compliquées et surtout changeant fréquemment.
  Grâce à la protection des données par défaut (privacy by default), quiconque traite de données personnelles doit permettre aux personnes concernées d'obtenir rapidement et facilement le plus haut niveau de protection possible. La législation sur la protection des données doit obliger chaque personne ou entreprise traitant des données personnelles à garantir par défaut le plus haut niveau possible de protection des données.

  Quelques exemples :

  Collecte des données
  - La granularité de la donnée doit être cohérente avec l'objectif du traitement. En assurance de personnes par exemple, dans la collecte de l'adresse, la rue peut être suffisante sans préciser le N°. De même concernant la date de naissance, il n'est pas forcément nécessaire de collecter le mois et le jour de naissance.

  Contrôle sur le partage des données
  - Mise en place d'un mécanisme de « whitelisting » : par défaut rien n'est partagé jusqu'à ce que la personne concernée active explicitement le partage d'une information.

  Stockage des données à caractère personnel
  - Le stockage de fichier contenant des données à caractère personnel identifiant et pouvant avoir un impact négatif pour les personnes concernées en cas de vol/perte des données (ex: pour contribuer à un vol d'identité) devrait être pseudonymisé anonymisé ou chiffré.
  - Les données médicales doivent être stockées par le responsable de traitement ou chez un hébergeur agréé.

  Transfert des données à des tiers
  - Si l'application prévoit de transférer les données personnelles à des tiers, une réflexion quant à l'opportunité de mettre en œuvre une pseudonymisation ou une anonymisation des données à caractère personnel avant le transfert à un tiers est un élément important à considérer dans le cadre de l'approche Privacy by Design.

  Mise à jour de l'application
  - Lorsqu'une mise à jour de l'application est disponible et appliquée, les paramètres de confidentialité configurés par la personne concernée doivent rester en l'état. Si de

nouveaux paramètres sont ajoutés à l'application, ceux-ci devraient appliquer par défaut le mode le plus restrictif de confidentialité pour les informations des utilisateurs.

5.11. Etude d'Impact sur la Vie Privée (EIVP) – Privacy Impact Assessment (PIA)

Pour tous les *traitements à risque*, le responsable de traitement devra conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.
Si l'organisme ne parvient pas à réduire ce risque élevé par des mesures appropriées, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Les « CNIL » pourront s'opposer au traitement à la lumière de ses caractéristiques et conséquences.
En juin 2012, la CNIL a publié un guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.
Ce guide a été révisé afin d'être plus en phase avec le projet de Règlement Européen sur la protection des données et propose une méthode plus rapide, plus facile à appliquer et plus outillée.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides :

- la démarche méthodologique
- et l'outillage (modèles et exemples).

Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.
Un PIA repose sur deux piliers :

- *les principes et droits fondamentaux, « non négociables »*, qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- *la gestion des risques sur la vie privée des personnes concernées*, qui permet de déterminer les mesures techniques et d'organisations appropriées pour protéger les données personnelles.

Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :

- *étude du contexte :* délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
- *étude des mesures* **:** identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
- *étude des risques* **:** apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
- *validation :* décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Jusqu'alors la législation européenne reposait sur la déclaration systématique de tous les traitements de données personnelles.
La nouvelle législation supprime cette obligation de déclaration pour favoriser le ciblage des traitements où une fuite ou une perte de contrôle des données produirait de graves conséquences pour les personnes concernées.

Ces traitements devront faire l'objet d'une analyse d'impact visant notamment à évaluer la probabilité et la gravité du risque de perte, de fuite, de mauvaise utilisation, ou de toute autre hypothèse de perte de contrôle des données traitées.
S'il s'agit de traiter un volume considérable de données à caractère personnel, que cela soit à un niveau régional, national, ou international, alors cette analyse d'impact est incontournable.
En fonction du résultat de l'évaluation, le responsable du traitement doit prendre toutes les mesures appropriées pour assurer la sécurité du traitement, et notamment se conformer à la législation en vigueur par rapport à sa situation telle que détaillée dans l'analyse d'impact.
Le Règlement dispose qu'une seule analyse d'impact puisse porter sur plusieurs traitements présentant le même niveau et le même type de risque.
Une analyse d'impact devra notamment comporter :
Une description détaillée des traitements envisagés, de leurs finalités et des intérêts légitimes poursuivis par le responsable
Une analyse de proportionnalité entre les spécifications du traitement et les finalités poursuivies
Une évaluation du risque pour les droits et libertés des personnes concernées
Les mesures d'atténuation du risque, les mécanismes visant à assurer la protection des données personnelles, les modes de preuve de conformité du traitement, la prise en compte des droits et des intérêts légitimes des personnes concernées
Par ailleurs, si un délégué à la protection des données a été désigné, il doit être consulté lorsque le responsable réalise une analyse d'impact.
Dans l'hypothèse d'un sous-traitant, ce dernier doit assister le responsable pour assurer le respect des obligations issues des analyses d'impact, y compris, si nécessaire, la consultation préalable de l'autorité de contrôle.
En effet, si l'analyse d'impact révèle que le risque posé par le traitement ne peut pas être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de leur mise en œuvre, le responsable doit consulter l'autorité de contrôle sur son projet.
Si l'autorité estime que le traitement viole la réglementation, elle le notifie par écrit au responsable, dans un délai de 8 semaines, prolongeable de 6 semaines en fonction de la complexité du traitement.
Ce délai ne commence à courir que lorsque l'autorité a reçu la totalité des informations qui lui sont nécessaires pour procéder à son évaluation.

Les autorités de contrôles peuvent établir, sous réserves, des listes de traitement automatique soumis ou exemptés d'analyse d'impact.

Certaines catégories de traitement ne sont pas concernées par cette analyse d'impact, il s'agit notamment des traitements couverts par le secret professionnel (médecin, avocat, hôpitaux…).

Enfin, le responsable de traitement doit mettre à jour son analyse d'impact au fil du temps, notamment quand une modification du traitement est susceptible de remettre en cause l'analyse d'impact initiale.

5.12. La sécurisation des transferts hors UE

La situation antérieure à l'adoption du Règlement Européen se résume ainsi :
Les transferts de données personnelles hors Union Européenne sont interdits sauf si le pays destinataire offre un niveau de protection identique à celui garanti dans l'UE (ces pays sont listés par les régulateurs).
Pour les autres pays, la vérification du niveau de protection suffisant se fait à travers :
La signature de clauses contractuelles type émanant de la Commission Européenne ou de la CNIL
L'adoption de Binding Corporate Rules (BCR)
Une décision d'autorisation de la Commission Européenne à effectuer le transfert.
Concernant les USA, les transferts étaient autorisés lorsque l'organisme destinataire avait adhéré au Safe Harbor, adhésion garantissant les principes posés par le Directive Européenne 95/46.

Avec l'adoption du projet Européen et la décision de la CJUE du 6 octobre 2015 invalidant le Safe Harbor, la situation est la suivante :

- Le principe est que les transferts requièrent une autorisation préalable.
- Toutefois peuvent être effectués sans autorisation les transferts :
  - Faisant l'objet d'une décision d'adéquation rendue par la Commission Européenne
  - Ayant les garanties appropriées suivantes :
    - clauses contractuelles type (Commission ou CNIL)
    - clauses contractuelles ad hoc validées par l'Autorité de contrôle
    - Binding Corporate Rules (BCR)

5.13. La formation des salariés

Dans le cadre du règlement, le délégué à la protection des données a, parmi ses prérogatives, d'assurer des sessions de formations / sensibilisation auprès du personnel participant aux opérations de traitements (article 37). Ces formations doivent être appropriées et spécifiques (article 47) à la population concernée.
Par ailleurs le comité (Comité Européen de la Protection des Données) a parmi ses obligations de promouvoir l'élaboration de programmes de formations sur le respect de la réglementation des données à caractère personnel.

6. Annexe 1 - Pack Assurance, Normes Simplifiées NS 16 et NS 56

I – Norme 16 sur la passation, la gestion et l'exécution des contrats d'assurance

La norme NS 16 est destinée à simplifier l'obligation de déclaration pour les catégories les plus courantes de traitements relative à la passation, à la gestion et à l'exécution des contrats d'assurance. Elle permet aux organismes d'assurance de procéder à un engagement de conformité auprès de la CNIL.
Le traitement des données personnelles doit respecter des règles qui concernent à la fois la finalité des traitements effectués sur ces données, la durée de conservation des données, les personnes habilitées à accéder aux données, l'information et les droits des personnes et les mesures de sécurité ainsi que le transfert des informations en dehors de l'Union Européenne.

1 Finalité poursuivies par le traitement
Tout traitement de donnée doit s'inscrire dans une logique prédéfinie. Sont donc exclus les traitements permettant de justifier une finalité de traitement a postériori. On distingue les finalités suivantes :
Finalité 1 : passation et la gestion des contrats :
• La passation des contrats
Il s'agit de l'étude des besoins spécifiques de chaque demandeur afin de proposer des contrats adaptés notamment dans le cadre du respect de l'obligation de conseil. Cela concerne aussi « l'examen, l'acceptation, le contrôle et la surveillance du risque ». On parle couramment de « l'appréciation des risques », de leur quantification et de leur assurabilité.
• La gestion des contrats
La gestion des contrats recouvre tout acte de gestion depuis la phase pré-contractuelle jusqu'à la résiliation du contrat. Il s'agit notamment de la tarification, de l'émission des documents pré-contractuels, contractuels et comptables, de l'encaissement des primes ou cotisations, de leur répartition éventuelle entre les coassureurs et les réassureurs, du commissionnement, de la surveillance des risques, et des autres opérations techniques nécessaires. Aucune décision refusant un contrat à une personne ne peut avoir pour seul fondement un traitement automatisé de données à caractère personnel.
Finalité 2 : l'exécution des contrats :
Il s'agit des opérations techniques nécessaires à la mise en œuvre des garanties et des prestations. Dans ce cadre, les données collectées sont relatives à la gestion des prestations, à la gestion des sinistres. Dans certains cas, il est possible que l'apériteur procède à la collecte de ces informations auprès des coassureurs et des réassureurs au moment de la souscription du contrat d'assurance ou lors de l'exécution des dispositions contractuelles.
Finalité 3 : l'élaboration des statistiques et études actuarielles.
Finalité 4 : l'exercice des recours et la gestion des réclamations et des contentieux.
Finalité 5 : l'exécution des dispositions légales, réglementaires et administratives en vigueur à l'exception de celles qui relèvent d'une formalité particulière prévue par la loi I&L
La réassurance peut potentiellement être concernée par l'une ou l'autre de ces finalités.

2 Catégories de données
Les données sont visées par un double principe: un **principe de proportionnalité** ou principe de limitation des quantités d'informations conservées et un **principe de pertinence** ou principe de bonne adéquation de ces informations avec la finalité poursuivie par le traitement.
Ces données peuvent être regroupées en **catégories de données**, par exemple :
- relatives à l'identification directe des individus : il peut s'agir des parties intéressées au contrat ou intervenantes au contrat qu'ils soient bénéficiaires, ayants droits, souscripteurs, exécuteurs de prestations de services, les professionnels de santé, …
- relatives à la situation familiale (ex : situation matrimoniale)
- relatives à la situation économique (ex :revenus)

- à la situation patrimoniale et financière (ex : toute information en lien avec le patrimoine mobilier ou immobilier)
- relatives à la situation professionnelle (ex : ou catégorie Socio Professionnelle de l'assuré ou toute information concernant l'employeur de l'assuré)
- liées à l'appréciation du risque (ex : détail décrivant un bien assuré)
- liées à l'exécution du contrat d'assurance (ex : numéro de chèque)
- liées à la gestion des sinistres et des prestations (ex : liées au contrat, au sinistres, à l'assuré ou à la victime)
- relatives à la détermination ou à l'évaluation des préjudices (ex : taux d'invalidité ou rapport d'expertise).
- relatives à la localisation des personnes ou des biens
- relatives à la vie personnelle (ex : situation de famille)
- relatives aux habitudes de vie (ex : activités sportives)
- en lien avec la santé

3 Conservation des données
La norme 16 impose des restrictions sur **les durées de conservation des données**.
La durée de conservation doit permettre de respecter les délais de prescriptions applicables en droit commun.
Il existe par ailleurs d'autres spécificités liées à la durée de conservation des données :
- Risques auto ou moto : l'assureur a une obligation de conserver les données détaillant les antécédents d'une personne en tant qu'assurée au cours des cinq dernières années.
- Des données relatives à la carte bancaire peuvent être conservées pour une finalité de preuve pendant 13 mois ou 15 mois pour les cartes de paiement à débit différé. Il est possible de conserver plus longtemps les données de la CB avec le consentement exprès du client. A noter que les données du cryptogramme visuel ne peuvent pas être stockées.
En lien plus direct avec la réassurance de personnes :
- Les données de santé: lorsque le contrat n'a pas été conclu, le responsable de traitement peut conserver les données de santé pendant **une durée maximale de 5 ans (2 années en archivage courant et 3 ans en archivage intermédiaire).**
- Les données collectées **en l'absence de conclusion d'un contrat peuvent être conservées pendant un délai de 3 ans maximum**

4 Destinataires
La norme NS16 impose par ailleurs des **restrictions quant aux destinataires ayant accès aux données à caractère personnel.**
Ces destinataires peuvent être habilitées à accéder aux données **dans le cadre de leurs missions habituelles**. Les **réassureurs** sont concernés.
Ces destinataires peuvent être habilitées à accéder aux données **en qualité de personnes intéressées au contrat** ou **en qualité de personnes habilitées au titre des tiers autorisés**.

5 Information et droits des personnes
La personne doit être informée, préalablement à la mise en œuvre du traitement de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, du transfert éventuel de ses données hors UE ainsi que des droits dont elle dispose au titre de la loi I&L.
À ce titre, elle dispose d'un droit d'accès, de rectification et d'opposition.

L'information des personnes sur les sites internet
Ces informations concernent moins spécifiquement la réassurance de personnes.
La norme précise :
Les données de connexion (date, heure, adresse Internet, protocole de l'ordinateur du visiteur, page consultée) peuvent être exploitées à des fins de mesure d'audience et d'assistance technique dans la mesure où elles ne soient pas recoupées avec d'autres traitements tels que les fichiers clients.
L'outil permettant de désactiver la traçabilité mise en œuvre par l'outil d'analyse de fréquentation doit être simple d'accès et aucune information relative aux internautes ayant décidé d'exercer leur droit d'opposition ne doit être transmise à l'éditeur de l'outil d'analyse de fréquentation.

Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a déjà été au préalable, de la finalité de toute action tendant à accéder à des informations déjà stockées dans son équipement terminal de communications électroniques ou à inscrire des informations dans cet équipement et des moyens dont il dispose pour s'y opposer.
Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord. »

6 Mesures de sécurité
On trouve dans la Norme 16 la description des mesures de sécurité suivantes :
Mesures de sécurité classiques
Le responsable du traitement prend **toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées.** Il définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme d'assurance. Cette politique décrit les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.
Les accès aux traitements de données nécessitent une **authentification des personnes** fiable et robuste.
Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits…).
Mesures de sécurité pour les sites internet
Le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques de cryptage.
Mesures de sécurité pour les données de santé
Le responsable de traitement s'engage à respecter les dispositions prévues par le code de bonne conduite annexé à la convention **AERAS** concernant la collecte et l'utilisation de données relatives à l'état de santé en vue de la souscription ou de l'exécution d'un contrat d'assurance.

7 Transferts de données hors UE
La norme prévoit les dispositions suivantes :
Certains transferts de données à caractère personnel peuvent être réalisés vers des pays tiers à l'UE et n'assurant pas un niveau de protection adéquat, lorsque:
• Il existe un niveau suffisant de protection de la vie privée, des droits et libertés des personnes ou que ces transferts sont juridiquement encadrés,
• Le responsable de traitement a clairement informé les personnes de l'existence d'un transfert de données vers des pays tiers, ou s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité, les données, les destinataires et les moyens mis en œuvre pour encadrer ce transfert,
• Les transferts sont réalisés lors de la gestion des actions ou contentieux liés à l'activité de l'entreprise (ex : constatation, exercice ou défense de ses droits en justice ou pour les besoins de défense des personnes concernées).
• Les transferts sont réalisés dans le cadre de l'exécution des contrats ou de la sauvegarde de la vie humaine pour la mise en œuvre des garanties d'assistance,
Les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique et d'un niveau de protection adéquat de type Safe Harbor, Clauses Contractuelles Types - dites CCT - ou règles internes d'entreprise - dites Binding Corporate Rules.
Tant que l'on reste dans le champ de la norme 16, aucune autorisation de la CNIL n'est nécessaire pour les transferts d'informations dans le cadre de la passation, la gestion et l'exécution des contrats. À défaut, ils doivent faire l'objet de déclarations auprès de la CNIL.

II - Norme 56 sur la gestion commerciale des clients et des prospects pour le secteur de l'assurance

La norme 56 est destinée à simplifier l'obligation de déclaration pour les catégories les plus courantes de traitements relative à la gestion commerciale des clients et prospects. Elle permet aux organismes d'assurance de procéder à un engagement de conformité auprès de la CNIL.
Le traitement des données personnelles doit respecter un certain nombre de règles qui concernent à la fois la finalité des traitements effectués sur ces données, la durée de conservation des données, les personnes habilitées à accéder aux données, l'information et les droit des personnes et les mesures de sécurité ainsi que le transfert des information en dehors de l'Union Européenne.

1 Finalités poursuivies par le traitement
Ces finalités peuvent être en lien direct ou indirect avec l'activité de transfert de risque par la **réassurance**.
Finalité 1 : les opérations relatives à la gestion des clients concernant un programme de fidélité ou le suivi de la relation client (réalisation d'enquêtes de satisfaction, regroupement des contrats pour un même client).
Finalité 2 : les opérations relatives à la prospection
Il s'agit de la gestion d'opérations techniques de prospection et de la sélection de personnes pour réaliser des actions de fidélisation, de prospection, de sondage, de test produit ou services et de promotion ou encore de la réalisation d'opérations de sollicitations, ou encore d'opérations permettant de cerner les attentes des clients ou le niveau de qualité de services.
Finalité 3 : l'élaboration de statistiques commerciales
Finalité 4 : la cession, la location ou l'échange des données relatives à l'identification des clients ou prospects pour améliorer le service au client en proposant des produits ou services permettant de réduire la sinistralité ou d'offrir un contrat ou une prestation complémentaire. Cela impose le strict respect des dispositions de la loi I&L, portant notamment sur l'information préalable des personnes (client ou prospect) et leur droit d'opposition.
Finalité 5 : l'organisation de jeux concours de loteries ou de toute opération promotionnelle.
Finalité 6 : la gestion des demandes de droit d'accès, de rectification et d'opposition.
Finalité 7 : la gestion des avis des personnes sur des produits, services ou contenus.

2 Catégories de données
Les données sont visées par un double principe: un **principe de proportionnalité** ou principe de limitation des quantités d'informations conservées et un **principe de pertinence** ou principe de bonne adéquation de ces informations avec la finalité poursuivie par le traitement. Les catégories de données sont sensiblement identiques aux catégories retenues pour la norme 16.
Les données de santé sont strictement exclues du périmètre de la norme 56.
À noter qu'un **code interne de traitement ne peut être le numéro d'inscription au répertoire national d'identification des personnes physiques** (numéro de sécurité sociale), ni le numéro de carte bancaire, ni le numéro d'un titre d'identité. Cela inclue également les données de localisation et de connexion, 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 de toute opération promotionnelle, et les données relatives aux contributions des personnes qui déposent des avis sur des produits, services ou contenus, notamment leur pseudonyme.

3 Durées de conservation
Des données relatives à la gestion de clients et de prospects :
• Les données des clients sont conservées le temps nécessaire pour la gestion de la relation commerciale.
• Les données **des clients utilisées à des fins de prospection commerciale** peuvent être conservées **pendant un délai de 3 ans à compter de la fin de la relation commerciale**.
• Les données **relatives à un prospect non client peuvent être conservées pendant un délai de 3 ans à compter** de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect.

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 doivent être supprimées ou archivées.
Pour l'exercice du droit d'accès ou de rectification, les données relatives aux pièces d'identité peuvent être conservées 1 an. En cas d'exercice du droit d'opposition, ces données peuvent être archivées 3 ans.
Concernant les listes d'opposition vis-à-vis des démarches de prospection: les informations permettant de prendre en compte le droit d'opposition de la personne concernée doivent être conservées au minimum 3 ans à compter de l'exercice de ce droit.

4 Destinataires
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, contrôle interne...)
• les sous-traitants dès lors que le contrat signé entre les sous-traitants et le responsable du traitement fait mention des obligations incombant aux sous-traitants en matière de protection de la sécurité et de la confidentialité des données.
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 organismes publics habilités, les arbitres, les médiateurs.
A noter que la réassurance peut directement ou indirectement être destinataire des données.

5 Information et droits des personnes
La personne doit être informée, préalablement à la mise en œuvre du traitement: de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, du transfert éventuel de ses données hors UE ainsi que des droits dont elle dispose au titre de la loi I&L.
Le recueil du consentement exprès et spécifique de la personne concernée est défini comme une manifestation de volonté libre et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées pour certaines finalités. L'acceptation des seules conditions générales d'utilisation n'est donc pas suffisante.
Dans le cas d'une collecte via un formulaire, le droit d'opposition ou le recueil du consentement préalable doit pouvoir s'exprimer par un moyen simple et spécifique, tel qu'une case à cocher.
Après la collecte des données, la personne concernée a le droit de s'opposer, sans frais, à ce que ses données soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.
Le responsable du traitement informe immédiatement de toute opposition tout autre responsable de traitement qu'il a rendu destinataire des données à caractère personnel qui font l'objet de l'opposition.

6 Utilisation d'un site internet
La norme 56 s'applique également dans le cas où le responsable de traitement utilise un site internet pour la gestion des clients et prospects.
L'exercice du droit d'opposition à l'analyse de sa navigation : l'outil permettant de désactiver la traçabilité mise en oeuvre par l'outil d'analyse de fréquentation doit rester simple d'accès et son installation doit être aisée pour tous les internautes. Aucune information relative aux internautes ayant décidé d'exercer leur droit d'opposition ne doit être transmise à l'éditeur de l'outil d'analyse de fréquentation.
Tout utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :
• **de la finalité** de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées
• **des moyens dont il dispose pour s'y opposer**.

7 Mesures de sécurité

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données, et notamment empêcher qu'elles soient **déformées** ou **endommagées** ou que des tiers non autorisés y aient accès.
Les accès aux traitements de données doivent nécessiter une authentification des personnes accédant aux données, au moyen par exemple d'un code d'accès et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification.
Dans le cas de l'utilisation d'un site internet, le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à rendre ces données incompréhensibles à toute personne non autorisée. Les pièces d'identité ne doivent être accessibles qu'à un nombre de personnes restreint et des mesures de sécurité doivent être mises en œuvre afin d'empêcher toute réutilisation détournée de ces données.

8 Transferts de données hors UE
Seules peuvent être transférées les données pertinentes au regard de la finalité poursuivie par le transfert.
La présente norme simplifiée couvre les transferts de données lorsqu'une des conditions suivantes est réunie :
• les transferts s'effectuent à destination d'un pays assurant un niveau de protection adéquat
• ils sont encadrés par les Clauses Contractuelles Types (dites CCT) ou par des règles internes d'entreprise (dites Binding Corporate Rules ou BCR) qui garantissent un niveau de protection suffisant
• ils correspondent à l'une des exceptions de l'article 69 de la loi I&L, limité à des cas de transferts ponctuels et exceptionnels.
Les transferts répétitifs, massifs ou structurels de données personnelles ne sont pas couverts par la présente norme et ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.

7. Annexe 2 – Le NIR (Numéro d'Inscription au Répertoire)

Acronymes
RNIPP : Registre National d'Identification des Personnes Physiques
NIR : Numéro d'Inscription au Répertoire (souvent appelé Numéro de Sécurité Sociale) d'identification des personnes physiques

La règlementation autour de l'utilisation du NIR concernant les acteurs qui font de l'assurance ou qui ont comme finalité la passation, la gestion et l'exécution des contrats d'assurance, de capitalisation, de réassurance et d'assistance est détaillée dans la norme simplifiée 16 sur la fiche pratique n°3.
L'utilisation du NIR est très précisément encadrée et répond à deux finalités.
La première finalité concerne :
Le traitement du NIR se justifie par la nécessité pour les assureurs de pouvoir communiquer vers la sécurité sociale (ou autres organismes sociaux) qui prennent déjà une partie des prestations en charge de couverture de santé, de retraite ….
L'autorisation de détention du NIR se justifie par la nécessité de travailler avec des sources d'information sur lesquelles le NIR figure (fiche de paie …)
Cependant, en aucun cas l'utilisation du NIR aux fins d'identification des doublons ou des homonymies ne fait partie de ces finalités.
La seconde finalité concerne la nécessité pour les organismes d'assurance d'accéder aux données du Registre National d'Identification des Personnes Physiques (RNIPP) dans certains cas très précis (comme la recherche d'assurés et de bénéficiaires …) via la base AGIRA. Y sont inscrites mensuellement les seules données personnelles des personnes dont les décès sont connus de l'INSEE suivantes : {NIR ; nom patronymique, prénoms ; sexe ; date et lieu de naissance ; date et lieu du décès ; numéro d'acte de décès}.
Le NIR et données les s'y rapportant de la bases AGIRA sont conservées par le responsable de traitement le temps nécessaire à l'exécution du contrat.
L'accès à ces données à caractère personnel est limité à un nombre restreint de personnes. Il dépend de la finalité des traitements mais permet l'exécution du contrat (gestion, intermédiaires, partenaires…). Il faut noter que les données issues des demandes auprès de la base AGIRA ne peuvent être traité que par un nombre limité de gestionnaires habilité à intervenir sur la gestion des contrats d'assurance vie.

Le responsable du traitement doit suivre la loi du 6 janvier 1978:
obligation d'information des personnes concernées par le traitement préalablement à sa mise en œuvre.
Respect des droits « informatique et liberté » en précisant notamment le service où les personnes concernées par le traitement peuvent exercer leur droit d'accès.

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité 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 (politique de sécurité, procédure d'identification des personnes accédant aux données, traçabilité des accès …), .

Sécurité et confidentialité

Les accès individuels à la base AGIRA s'effectuent après authentification mutuelle du système hébergeant le traitement et de la personne concernée par le biais de certificats délivrés par le réseau d'accès aux données de l'assurance et de la messagerie sécurisée (RADAMESS). L'identification des machines connectées au traitement est également faite par des certificats de même nature.
Le certificat doit être nominatif et les mesures appropriées doivent être prises de manière à garantir qu'il ne sera utilisé que par son titulaire.
Les organismes d'assurances, institutions de prévoyance et leurs unions, et les mutuelles et leurs unions conservent l'historique des requêtes ponctuelles effectuées sous leur responsabilité et pourront accéder aux interrogations conservées par l'AGIRA. Celle-ci garde une trace de toute interrogation pendant un an.

Toutes les connexions au traitement de données à caractères personnel font l'objet d'un chiffrement. Tous les envois dématérialisés entre l'INSEE et l'AGIRA font l'objet d'un chiffrement dont la clé est fournie sous pli séparé, en recommandé, avec accusé de réception. Les transmissions de la clé et des données se font successivement, en deux plis distincts, les données n'étant envoyées qu'après retour à l'INSEE de l'accusé de réception du courrier contenant la clé.

8. Annexe 3 – La lutte contre la fraude

Périmètre

L'autorisation unique n°39 finalise le pack assurance avec les traitements mis en œuvre dans le cadre de la lutte contre la fraude en assurance. Cette AU se veut la plus large possible et concerne aussi bien la fraude interne et externe. Son objectif est de permettre l'utilisation des données par les assureurs pour lutter contre la fraude et de respecter les principes de la loi informatique et libertés et la doctrine de la Commission.
La définition qui a été retenue pour la fraude est la suivante « tout acte ou omission commis intentionnellement par une ou plusieurs personnes afin d'obtenir un avantage ou un bénéfice de façon illégitime, illicite ou illégal ».

Finalités poursuivies par le traitement

Finalités :
l'analyse et la détection des actes 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.

L'employeur peut également procéder à des **requêtes individuelles et ponctuelles** dans le cadre de son pouvoir d'enquête interne, sur les données collectées au titre de la gestion administrative du personnel.

Les interconnexions sont possibles si elles émanent du responsable de traitement ou du groupe auquel il appartient et sont possibles uniquement en matière de :
gestion commerciale de clients et de prospects (NS 56) ;
passation, gestion et exécution des contrats (NS 16) ;
lutte contre le blanchiment et le financement du terrorisme (AU003) ;
collecte et traitement des données d'infractions, de condamnations et mesures de sûreté (AU 32) ;
gestion des relations contractuelles avec les intermédiaires, les prestataires, les sous-traitants, les délégataires, et les partenaires.

Les requêtes ou **alertes automatiques font l'objet d'une analyse manuelle** par le personnel habilité de l'organisme ou du groupe. La personne concernée doit pouvoir présenter ses observations, si une décision produisant des effets juridiques est prise à son égard.

Catégories de données

Données à disposition de l'assureur :
Données relatives à **la passation, la gestion et de l'exécution des contrats (NS 16) :**
Données relatives à **la gestion et au suivi de la relation commerciale (NS 56) :**
Le **NIR**
Données plus spécifiques à la problématique de la fraude :
Données relatives **aux infractions, condamnations et mesures de sûreté (AU 32) concernant :** les personnes / les circonstances de l'infraction / les suites données à la constatation de l'infraction
Données **de journalisation des accès aux traitements (NS 16, NS 56, AU 31 et AU 32)** (badgage, absences, rémunération des salariés …)
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.
Données relatives aux **anomalies, incohérences et signalement** pouvant révéler une fraude.
Données relatives aux **investigations, à l'instruction** du dossier de fraude et à l'évaluation du **périmètre** de la fraude.

Données d'**identification des personnes** intervenant dans la détection et la gestion de la fraude. (enquêteurs, anonymat des personnes…)

Durée de conservation

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. Passé ce délai, si l'alerte n'est pas qualifiée de « pertinente », les données doivent être supprimées immédiatement.
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 puis elles sont archivées.

Destinataires

Il existe des listes précises de destinataires pour ces données.
Les destinataires classiques pour la gestion de la fraude interne et externe sont par exemple les DRH, représentant du personnel, gestionnaire de sinistres, enquêteurs, personnels habilité des sous-traitants…
Et ceux directement concernés par la fraude (autres organismes d'assurance, autorité judiciaires, organismes tiers autorisés par disposition légale …)
La communication de ces données ne peut en aucun cas donner lieu à la création d'un fichier concernant les données relatives aux fraudes et mutualisé entre les destinataires.

Information des personnes

Il existe une obligation d'information générale conformément aux dispositions de l'article 32 de la loi informatique et libertés.
les personnes sont informées du fait que le responsable de traitement met en œuvre un dispositif ayant pour finalité la lutte contre la fraude pouvant, notamment, conduire à l'inscription sur une liste de personnes présentant un risque de fraude
après un délai de 6 mois d'investigation, en cas de confirmation de l'anomalie et de décisions produisant des effets juridiques, la personne susceptible d'être inscrite sur une liste de personnes présentant un risque de fraude, doit être informée individuellement par écrit des dites conséquences en lui donnant la possibilité de présenter ses observations.

Sécurité et confidentialité

Le responsable du traitement :
prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données ansi que toutes les mesures nécessaires pour assurer la maintenance du matériel
définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme d'assurance (droit d'accès spécifiques pour accéder aux données, système de traçabilité, audit …).

Transfert des données hors de l'union européenne

Les transferts sont possibles dans les conditions prévues par la loi "Informatique et libertés". Ils doivent être pertinents au regard de la finalité du traitement et être effectué uniquement si
Le transfert est réalisé vers un pays offrant un niveau de protection adéquat, ou
Il est encadré par des Clauses Contractuelle Type (CCT) ou des règles d'entreprise (BCR), ou
Effectué de façon ponctuelle et exceptionnelle dans le cadre de l'une de exception de de la loi I&L art.39.

9. Annexe 4 – Rédacteurs

Contributeurs à la rédaction :

- Marie SCHALLIER, MutRé
- Marvin DEWKURUN, SCOR
- Delphine LABOJKA, SCOR
- Medhi HIMEUR, PARTNER RE
- Benoît AUDOYE, SWISS RE
- Xavier DEBRAS, SWISS RE
- Arnaud VERREY, CCR
- Jean-Pierre MLYNARCZYK, GEN RE
- Gurvan LE RHUN, RGA
- Johann LAUNAY, HANNOVER RE
- Jean MODRY, HANNOVER RE