ASSOCIATION FRANÇAISE DE L'ASSURANCE

Fédération Française des Sociétés d'Assurances

GEMA ASSUREURS MUTUALISTES

CNIL
Commission Nationale de l'Informatique et des Libertés

PACK CONFORMITE ASSURANCE

- Un besoin de sécurité juridique
- Des normes générales
- Une simplification administrative
- Des normes durables

ASSOCIATION FRANÇAISE DE L'ASSURANCE

Fédération Française des Sociétés d'Assurances

GEMA ASSURANCES MUTUALISTES

CNIL
Commission Nationale de l'Informatique et des Libertés

Pourquoi un pack de conformité ?

- Un « nouvel » outil de **pilotage de la conformité** pour les professionnels de l'assurance

- Une démarche moderne et pragmatique :
  - ✓ une réponse opérationnelle aux besoins des professionnels concernant la loi I&L
  - ✓ une collaboration étroite entre la CNIL et les assureurs pour la mise en place d'outils juridiques de simplification ou d'allégement des formalités (NS et AU) et de bonnes pratiques adaptées à l'assurance (fiches pratiques)

- Le pack est aussi un moyen d'anticiper sur les changements attendus avec le projet de règlement européen sur la protection des données :
  - ✓ les responsables de traitement bénéficieront d'une simplification des formalités au profit d'une relation plus dynamique avec le régulateur
  - ✓ pour cette raison, la capacité à rendre compte de la mise en conformité avec la loi devient un enjeu essentiel

ASSOCIATION FRANÇAISE DE L'ASSURANCE

Fédération Française des Sociétés d'Assurances

GEMA ASSURANCES MUTUALISTES

CNIL
Commission Nationale de l'Informatique et des Libertés

Méthodologie : le point de vue de la profession

- Des échanges réguliers entre la CNIL et toutes les familles d'organismes d'assurance et des travaux préparatoires au sein des familles elles-mêmes

- Des échanges permettant aux assureurs de mieux expliquer leurs métiers et la diversité des obligations réglementaires encadrant leur activité

  - ✓ les assureurs ne font pas des traitements excluant une personne d'un droit ou d'un contrat sans fondement législatif ou réglementaire

- Une attention particulière a été apportée aux **données de santé** qui font l'objet d'un encadrement (cf. Convention AERAS et Code de bonne conduite).

ASSOCIATION FRANÇAISE DE L'ASSURANCE

Fédération Française des Sociétés d'Assurances

GEMA ASSUREURS MUTUALISTES

CNIL
Commission Nationale de l'Informatique et des Libertés

Présentation du Pack conformité

Partie 1 :

- Une norme simplifiée NS 16 actualisée et relative à la passation, gestion et exécution des contrats d'assurance
- Une norme simplifiée NS 56 relative à la gestion commerciale des clients et prospects prenant appui sur la norme simplifiée NS 48 actuellement en vigueur qui exclut certains secteurs d'activité dont les professionnels de l'assurance.

Partie 2 :

- Une autorisation unique AU 31 relative à la collecte et au traitement du numéro d'inscription au répertoire national des personnes physiques (NIR), et à la consultation du RNIPP
- Une autorisation unique AU 32 concernant les traitements de données relatifs aux infractions, condamnations et mesures de suretés
- Une autorisation unique AU 39 relative aux traitements mis en œuvre dans le cadre de la lutte contre la fraude.

La refonte de la NS 16

- Concerne les organismes d'assurance, de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance. Sont donc bien inclus dans le périmètre les mutuelles et les institutions de prévoyance, les courtiers et agents généraux d'assurance.

- **Finalités :**

  - ✓ Des finalités qui englobent l'acceptation et la surveillance du risque, l'exercice des recours, la gestion des réclamations et contentieux.
  - ✓ Les finalités relatives à la gestion de la relation commerciale sont reportées dans la NS56.

La refonte de la NS 16

- **Les catégories de données :**

✓ La norme 16 ancienne, visait une liste des données dont certaines étaient obsolètes (situation militaire)

✓ Nécessité d'acter des catégories de données plutôt qu'une liste de données compte tenu de la diversité des données traitées selon les types de produits concernés

✓ Prise en compte des données d'appréciation du risque, de localisation des personnes ou des biens en relation avec les risques assurés

La refonte de la NS 16

- La nouvelle version vient désormais préciser le cadre juridique relatif à la collecte des **données de santé**

  - ✓ Recueil du consentement exprès de la personne concernée sauf s'il ne peut être matériellement ou juridiquement recueilli, ou que l'organisme est soumis à une obligation légale de recueillir ces informations.

La refonte de la NS 16

❖ **Les durées de conservation** :

❑ Principe général : cohérence entre les durées de conservation et les délais de prescription

❑ Précisions sur :

✓ les données en l'absence de conclusion d'un contrat d'assurance
✓ les données relatives aux cartes bancaires collectées lors de l'exécution du contrat d'assurance :

- suppression au-delà du délai de contestation de la transaction,
- des exceptions sont prévues à titre probatoire ou avec le consentement exprès de la personne concernée,
- interdiction de conserver le cryptogramme.

La refonte de la NS 16

❖ **L'information des personnes :**

✓ Un nouvel article est intégré avec un paragraphe sur la communication au public en ligne (site internet).

❖ **Les mesures de sécurité :**

✓ Un nouvel article décrit les obligations en matière de sécurité :

- une politique de sécurité à formaliser (sur les mesures mises en œuvre) adaptée aux risques et à la taille de l'organisme d'assurance
- un accès aux données sous authentification et traçabilité des accès
- un renforcement des dispositions sur la sécurité des données de santé des assurés (code de bonne conduite annexé à la convention AERAS)
- des mesures techniques à prendre afin de rendre incompréhensibles à toute personne non autorisée à y accéder les données transitant sur des canaux de communication non sécurisées

La refonte de la NS 16

- **Un article relatif à l'appréciation du risque (article 7) :**
  - Il n'est pas possible de prendre une décision de refus automatisée et sans la possibilité pour la personne concernée de présenter ses observations

- **Deux nouveaux articles ont été ajoutés :**
  - Sur le transfert de données vers l'étranger (article 9)
  - Sur l'utilisation d'un service de communication au public (article 10)

NS 56 : pour la gestion commerciale

❑ La NS 48 n'est pas applicable au secteur de l'assurance. Les assureurs ont été demandeurs d'une norme similaire, c'est l'objet de la NS 56.

❖ **Finalités :**

❑ Permettant notamment de réaliser des opérations relatives à :

- ✓ la gestion des clients (suivi de la relation client, enquêtes de satisfaction, …)
- ✓ la prospection (sélection de personnes, tests de produits ou services, actions de fidélisation…)
- ✓ des sollicitations :

  - élaboration de statistiques commerciales,
  - cession, location ou échange de données d'identification de clients et de prospects,
  - organisation de jeux-concours, loteries ou toute opération promotionnelle à l'exclusion des jeux d'argent et de hasard en ligne.

NS 56 : pour la gestion commerciale

- Quelques précisions importantes :

  - ✓ Il est nécessaire qu'un groupe d'assurance puisse suivre sa relation client de manière exhaustive en tenant compte des contrats qu'il a souscrits en assurance vie ou non vie.
  - ✓ Dans le cadre du suivi de la relation client, le regroupement des contrats pour un même client au sein du groupe auquel appartient l'organisme est pris en compte.

- La cession, la location ou l'échange de données relatives à l'identification de clients ou prospects :

  - ✓ limitée à des propositions de produits ou services permettant de réduire la sinistralité ou d'offrir un contrat ou une prestation complémentaire.

NS 56 : pour la gestion commerciale

- **Les catégories de données :**
  - Celles de la NS 48 adaptées aux besoins de l'activité (ex: produits ou services et non achats de biens).
  - 2 spécificités pour l'assurance :
    - ✓ sont exclues les données de santé
    - ✓ les données de facturation, règlement, impayés… sont déjà prévues dans la NS16 donc absentes de NS 56

- **Les durées de conservation des données :**
  - Concernant les données relatives à la gestion de clients et de prospects
  - Les données permettant d'établir la preuve d'un droit ou d'un contrat, ou conservées au titre du respect d'une obligation légale, peuvent être archivées conformément aux dispositions en vigueur (code des assurances, code de la mutualité, code de commerce, code civil et code de la consommation)

NS 56 : pour la gestion commerciale

- **Les mesures de sécurité :**

- Les pièces d'identité ne doivent être accessibles qu'à un nombre restreint de personnes et des mesures doivent être mises en œuvre contre tout détournement

- Pour les autres dispositions, les mesures de sécurité sont identiques à celles de la NS 16.

AU 31 NIR et RNIPP

- Abrogation de la délibération n°2008-579 (AU 18 Accès au RNIPP pour la recherche de bénéficiaires et assurés décédés)
- Cette AU concerne également l'AGIRA

❖ **Finalités :**

- Collecte et traitement du NIR pour les activités d'assurance visées par la réglementation (maladie, retraite supplémentaire, invalidité, maternité, perte d'emploi et pertes d'exploitation…)
- Accès au RNIPP tel que le prévoyait l'AU 18

AU 31 NIR et RNIPP

❖ **Destinataires :**

❑ Pour les données relatives aux personnes décédées (RNIPP) : un nombre limité de gestionnaires habilités, adapté à la taille du portefeuille et disposant de certificats individuels

❖ **Les mesures de sécurité :**

❑ Une politique de sécurité à formaliser (sur les mesures mises en œuvre)

❑ Accès aux données sous authentification et traçabilité des accès

❑ Les mesures spécifiques prévues dans l'AU18 sont intégrées à l'AU 31

AU 32 Les traitements de données d'infractions de condamnations ou mesures de sûreté

- Des données qui peuvent être recueillies lors de la déclaration du risque ou du traitement d'un sinistre
- Des données qui peuvent être nécessaires à l'organisme dans la gestion d'un contentieux pour la constatation, l'exercice ou la défense de ses droits en justice, ou la défense des personnes concernées

❖ **Finalités :**

- Un traitement de ces données uniquement dans le cadre des finalités de la NS16 ou pour assurer la constatation, l'exercice ou la défense des droits en justice, de l'entreprise ou la défense des personnes concernées
- Pas de mutualisation des informations entre les organismes d'assurance à l'exclusion de l'AGIRA

ASSOCIATION FRANÇAISE DE L'ASSURANCE

Fédération Française des Sociétés d'Assurances

GEMA ASSUREURS MUTUALISTES

CNIL
Commission Nationale de l'Informatique et des Libertés

AU 32 Les traitements de données d'infractions de condamnations ou mesures de sûreté

❖ **Les catégories de données :**

- ❑ Identification des personnes, le cas échéant les données issues des PV, les décisions judiciaires ou administratives, les enquêtes judiciaires
- ❑ Les circonstances de l'infraction
- ❑ Les suites données à la constatation de l'infraction notamment condamnations ou mesures de sureté

❖ **Les mesures de sécurité :**

- ❑ Identiques à la NS16

AU 39 La lutte contre la fraude

❖ **Définition de la fraude :**

*« Un **acte ou omission** commis **intentionnellement** par une ou plusieurs personnes afin d'obtenir un **avantage ou un bénéfice** de façon **illégitime, illicite ou illégale** ».*

❑ La lutte contre la fraude, une priorité en terme de protection des assurés, équité, dissuasion et maitrise des risques.

AU 39 La lutte contre la fraude

❖ **Périmètre :**

- ❑ Concerne la lutte contre la fraude interne (salariés, agents généraux, intermédiaires..) et externe (personnes parties, intéressées ou intervenantes au contrat).
- ❑ Uniquement dans le cadre des activités relatives à la passation, la gestion et l'exécution des contrats d'assurance, capitalisation, réassurance et assistance.
- ❑ Ne concerne pas la lutte anti-blanchiment qui a donné lieu à une autorisation unique multisectorielle AU-003 du 16 juin 2011

AU 39 La lutte contre la fraude

❖ **Finalités :**

- ❑ Analyse et détection des actes présentant une anomalie, une incohérence ou ayant fait l'objet de signalements
- ❑ Gestion de ces alertes
- ❑ Possibilité de constituer des listes de personnes d'actes susceptibles d'être constitutifs d'une fraude
- ❑ Gestion des conséquences éventuelles pour le fraudeur avéré
  - ✓ Procédures, application des dispositions contractuelles, législatives et réglementaires
- ❑ Certains outils peuvent permettre sur la base de requêtes de produire des alertes
  - ✓ Pas de décision produisant des effets juridiques pour une personne sur le seul fondement d'un traitement automatisé

AU 39 La lutte contre la fraude

- L’entreprise peut accéder ponctuellement et individuellement aux données de gestion administrative du personnel (enquête interne).

- Des interconnexions sont possibles entre les traitements des données NS 16, NS 56, LAB (tel que prévu dans AU 003), AU 32 et les données de gestion dans le cadre des relations avec les intermédiaires, sous-traitants, délégataires et partenaires.

AU 39 La lutte contre la fraude

❖ **Les catégories de données :**

- ❑ Sont concernées les données du « pack assurance » : NS 16, NS 56, AU 32, et le NIR en conformité avec l'AU 31
- ❑ La journalisation des accès aux traitements relevant de ces normes
- ❑ Les données issues de la gestion administrative du personnel
- ❑ Les données de gestion, d'investigations et l'instruction des dossiers de fraude potentielle et / ou avérée
- ❑ Les anomalies, incohérences et signalements
- ❑ Les données d'identification des personnes intervenant dans la détection et la gestion de la fraude

AU 39 La lutte contre la fraude

❖ **Les durées de conservation des données :**

❑ Toute alerte non pertinente est supprimée sans délai :

✓ Délai de 6 mois pour qualifier une alerte
✓ Suppression de l'alerte non qualifiée dans ce délai

❑ Si l'alerte est pertinente :

✓ Conservation des données 5 ans après clôture du dossier de fraude
✓ En cas de procédure judiciaire, conservation jusqu'au terme de la procédure et archivage

❑ La personne inscrite sur la liste des fraudeurs présumés est supprimée après le délai de 5 ans à compter de son inscription

AU 39 La lutte contre la fraude

❖ **Les destinataires :** dans la limite de leurs attributions et pour ces finalités

❑ Fraude interne

- ✓ personnes habilitées RH, conseil de discipline et représentants du personnel

❑ Fraude interne et externe

- ✓ personnels en relation avec clientèle, gestionnaires
- ✓ entités du Groupe (si concernées)
- ✓ personnels habilités de l'entreprise ou externes (sous-traitants, enquêteurs, experts..)
- ✓ organismes concernés par une fraude (assureurs, intermédiaires, organismes sociaux, professionnels, tiers autorisés)
- ✓ victimes ou leurs représentants
- ✓ autorités

❑ Pas de création d'un fichier de données relatives aux fraudes entre les destinataires

AU 39 La lutte contre la fraude

❖ **L'information des personnes :**

❑ **Information générale**

✓ Sur l'existence d'un dispositif de lutte contre la fraude et de l'inscription possible sur une liste de personnes présentant un risque de fraude

❑ **Fraude interne**

✓ Information individuelle des salariés (règlement intérieur ou tout autre support de communication)

✓ Dans les documents contractuels ou autre support pour les prestataires, mandataires, intermédiaires, élus des organismes…

AU 39 La lutte contre la fraude

❖ **Fraude externe :**

❑ Au moment de la souscription dans les documents contractuels ou tout autre support échangé lors de l'exécution du contrat

❖ **Information spécifique :**

❑ Après 6 mois d'investigations :

✓ si l'anomalie est confirmée

✓ si les décisions prises produisent des effets juridiques pour la personne :

- Information de la personne sur les conséquences (ex : refus du règlement d'une prestation, résiliation du contrat…) en lui donnant la possibilité de présenter ses observations
- Pas d'information lors de l'inscription sur une liste de surveillance

Entrée en vigueur des normes

Les organismes disposent de délais de mise en conformité :

Exemple : AU 39 = 31 juillet 2016

Tout projet de traitement qui excèderait le cadre des NS ou AU doit faire l'objet d'une demande spécifique