

Date de publication sur legifrance: 26/02/2014

**Commission Nationale de l'Informatique et des Libertés**

**DELIBERATION n°2014-015 du 23 janvier 2014**

**Délibération n° 2014-015 du 23 janvier 2014 portant création d'une autorisation unique concernant les traitements de données à caractère personnel relatifs aux infractions, condamnations ou mesures de suretés mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance, les intermédiaires d'assurance, et par l'AGIRA.**

AU-032

La Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code des assurances ;

Vu le code civil ;

Vu le code général des impôts ;

Vu le code de la mutualité ;

Vu le code pénal ;

Vu le code de procédure pénale ;

Vu le code de la route ;

Vu le code rural ;

Vu le code de la santé publique ;

Vu le code de la sécurité sociale ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 25-1-3° et 69 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Monsieur Jean-Paul AMOUDRY, commissaire, en son rapport, et Monsieur Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations.

Formule les observations suivantes :

Les organismes d'assurance, de capitalisation, de réassurance, d'assistance, les intermédiaires d'assurance effectuent dans le cadre de la passation, de la gestion et de l'exécution des contrats d'assurance, de capitalisation, de réassurance, et d'assistance, des traitements de données relatifs aux infractions, condamnations ou mesures de sûreté à plusieurs niveaux : soit au moment de la souscription du contrat d'assurance, soit au cours de son exécution ou dans le cadre de la gestion des contentieux.

Lors de la souscription du contrat, les traitements des données d'infractions, de condamnations et les mesures de sûreté, permettent d'évaluer le risque des contrats en ayant une connaissance globale du client et notamment des antécédents de l'assuré. En effet, en assurance de responsabilité automobile, les dispositions de l'article A.335-9-2 du Code des assurances limite les majorations qu'un assureur serait incité à appliquer en fonction d'un certain nombre d'infractions.

Ces informations sont obtenues par l'assureur lors de la déclaration du risque (article L.113-2-2° du Code des assurances) en posant des questions fermées à l'assuré. En matière d'assurance professionnelle des mandataires sociaux, l'assureur peut être amené à demander au futur assuré s'il a fait l'objet de condamnation ou de poursuite devant une juridiction pénale puisque ces éléments lui permettront d'évaluer son risque assurantiel.

Au cours de la vie du contrat, ces données permettront d'accorder ou non une garantie aux assurés ou d'indemniser les tiers victimes. En effet, pour procéder au règlement des sinistres et des prestations, il peut s'avérer nécessaire de vérifier les faits qui ouvrent droit à garantie.

Ainsi, la connaissance des circonstances d'un vol est nécessaire pour vérifier si les conditions de garantie sont réunies et le dépôt d'une plainte peut être une condition d'indemnisation. Certaines garanties vol peuvent être limitées aux cas d'effraction et conformément aux dispositions contractuelles applicables, l'assuré devra rapporter la preuve de l'effraction. Par ailleurs, les dispositions de l'article L211-10 du code des assurances obligent l'assureur à informer la victime qu'elle peut obtenir de sa part, sur simple demande, une copie du procès-verbal. Ainsi, les assureurs de véhicules impliqués dans un accident de la circulation, reçoivent les procès verbaux de police, dans un but d'accélération des procédures d'indemnisation, selon une procédure dénommée « transpv ».

Enfin, dans le cadre de la gestion des contentieux, l'organisme d'assurance doit être en mesure d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou la défense des personnes concernées.

Par ailleurs, l'Association pour la gestion des informations sur le risque en assurance (AGIRA) gère un fichier des résiliations automobiles qui permet aux sociétés d'assurances, de vérifier les antécédents d'un futur assuré lors de la souscription d'un contrat d'assurance automobile. A ce titre, elle collecte des données d'infractions relatives aux caractéristiques des sinistres.

Dès lors, ces traitements relèvent du 3° du I de l'article 25 et 69 de la loi du 6 janvier 1978 modifiée et doivent, à ce titre, être autorisés par la CNIL.

En vertu de l'article 25-II de la loi du 6 janvier 1978 modifiée, la commission peut autoriser par une décision unique une catégorie de traitements répondant aux mêmes finalités, portant sur des catégories de données identiques et ayant les mêmes catégories de destinataires. Il en résulte que le responsable d'un traitement conforme à cette décision unique d'autorisation pourra déclarer son

traitement en adressant à la commission un engagement de conformité par lequel il s'engage à respecter les termes de la décision de la CNIL.

Décide :

D'adopter une autorisation unique pour les traitements automatisés ou non de données à caractère personnel relevant de l'article 25-1-3° ;

Les organismes mentionnés ci-dessous qui souhaiteront se référer à la présente autorisation unique adresseront à cette fin, à la Commission un engagement de conformité pour leurs traitements qui répondent strictement aux conditions définies ci-dessous ;

Tous les traitements qui ne sont pas strictement conformes à la présente autorisation unique devront faire l'objet d'une demande d'autorisation spécifique présentant et expliquant les différences entre le traitement envisagé et l'autorisation unique.

#### Article 1 : Champ d'application

Sont concernés les organismes d'assurance, de capitalisation, de réassurance, d'assistance les intermédiaires d'assurance, ci après désignés, les « organismes d'assurance » et l'AGIRA.

#### Article 2 : Finalités du traitement

Sont autorisés les seuls traitements de données à caractère personnel ayant pour finalités la passation, la gestion et l'exécution des contrats d'assurance, de capitalisation, de réassurance, et d'assistance nécessitant :

- la collecte et le traitement de données relatives aux infractions, condamnations ou mesures de sûreté prévus par les dispositions légales, réglementaires et administratives en vigueur.
- Ces traitements interviennent également dans le cadre des contentieux liés à l'activité et permettant notamment à l'entreprise d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou la défense des personnes concernées.

Ces traitements ne peuvent en aucun cas faire l'objet d'une mutualisation des informations entre les organismes d'assurance à l'exclusion de l'AGIRA.

#### Article 3 : Catégories de données à caractère personnel traitées

Peuvent être collectées, dans le cadre des finalités décrites à l'article 2, les données relatives aux infractions, condamnations et mesures de sûreté des personnes parties, intéressées ou intervenantes au contrat, à savoir :

##### a) Concernant les personnes :

Les données d'identification : nom et prénom(s), date et lieu de naissance.

Les coordonnées postales.

Le cas échéant, les données issues des procès verbaux de police ou de gendarmerie, les décisions judiciaires ou administratives et les enquêtes judiciaires.

##### b) Concernant les circonstances de l'infraction :

Les faits constatés.

La présence de témoins, leur identification et leurs témoignages.

c) Suites données à la constatation de l'infraction :

Saisine ou absence de saisine.

Classement sans suite.

Engagement de poursuite.

Condamnations.

Mesures de sûreté.

Article 4 : Durées de conservation des données

Les données collectées sont conservées par le responsable de traitement pour la durée nécessaire à l'exécution du contrat dans les cas visés à l'article 2.

Ces données sont ensuite archivées conformément aux durées prévues par les dispositions des articles L.114-1 et suivants du code des assurances, de l'article L.932-13 du code de la sécurité sociale et des dispositions du code civil relatives à la prescription.

Article 5 : Destinataires des informations et personnes habilitées à traiter les données

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

a. dans le cadre des missions habituelles qui leurs sont assignées et dont ils doivent répondre :

- les personnels chargés de la passation, la gestion et l'exécution des contrats;
- les délégataires de gestion, les intermédiaires d'assurance, les organismes d'assurance chargés dans le cadre d'un contrat de partenariat de gérer les contrats d'assurance du responsable de traitement ;
- les prestataires agissant sur ordre du responsable de traitement dans le cadre des activités prévues à l'article 2 ;
- les sous-traitants, ou les entités du groupe d'assurance auquel appartient le responsable de traitement dans le cadre de l'exercice de leurs missions ;
- s'il y a lieu les organismes d'assurance des personnes impliquées ou offrant des prestations complémentaires ;
- s'il y a lieu les co-assureurs et réassureurs ainsi que les organismes professionnels et les fonds de garanties ;
- les personnes intervenant aux contrats tels que les avocats, experts, auxiliaires de justice et officiers ministériels, curateurs, tuteurs, enquêteurs,
- les organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux ;

b. en qualité de personnes intéressées au contrat :

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

c. en qualité de personnes habilitées au titre des tiers autorisés :

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

#### Article 6 : Information des personnes concernées

Le responsable du traitement doit, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée, informer les personnes concernées préalablement à la mise en œuvre du traitement:

- de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant
- de la finalité poursuivie par le traitement auquel les données sont destinées ;
- du caractère obligatoire ou facultatif des réponses
- des conséquences éventuelles, à son égard, d'un défaut de réponse,
- des destinataires ou catégories de destinataires des données ;
- de l'existence des droits d'accès, de rectification et d'opposition
- le cas échéant de transfert de données personnelles à destination d'un Etat non membre de l'Union Européenne.

Le droit d'accès défini au chapitre V de la loi du 6 janvier 1978 modifiée s'exerce auprès du ou des services que le responsable du traitement aura désignés.

#### Article 7 : Mesures de sécurité

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.

Le responsable de traitement définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme d'assurance. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.

Les accès aux traitements de données nécessitent une authentification des personnes accédant aux données, au moyen d'un identifiant et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification de même fiabilité.

Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits...).

## Article 8 : Transferts de données vers l'étranger

Les transferts de données à caractère personnel réalisés vers des pays tiers à l'Union Européenne qui ne sont pas membres de l'Espace économique européen, peuvent être effectués lorsque l'une des conditions suivantes est réunie :

- les transferts s'effectuent à destination d'un pays reconnu par une décision de la Commission européenne comme assurant un niveau de protection suffisant, ou d'une entreprise américaine ayant adhéré aux principes du « Safe Harbor » ; ou,
- le traitement garantit un niveau suffisant de protection de la vie privée ainsi que les droits et libertés fondamentaux des personnes par la mise en œuvre des clauses contractuelles types adoptées par la Commission européenne ou par l'adoption de règles internes d'entreprise dénommées « BCR » dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant ; ou,
- ces transferts sont réalisés dans le cadre de l'exécution des contrats ou pour la mise en œuvre des garanties (article 69, 1°, 5°, 6° de la loi « Informatique et Libertés »), ou lors de la gestion des actions ou contentieux liés à l'activité et permettant notamment à l'entreprise d'assurer la constatation, l'exercice ou la défense de ses droits en justice ou pour les besoins de défense des personnes concernées (article 69, 3° de la loi « Informatique et Libertés »).

Le recours à ces exceptions de l'article 69 n'est possible que pour les transferts dont le champ d'application est limité à des cas de transferts ponctuels et exceptionnels. Ainsi, les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique « BCR », clauses contractuelles types ou Safe Harbor).

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

## Article 9 : Dispositions transitoires

Les traitements de données à caractère personnel dont la mise en œuvre est intervenue avant la publication de la présente délibération disposent d'un délai de 18 mois à compter de cette publication pour adresser à la Commission un engagement de conformité avec les dispositions de l'AU 032.

La présente délibération sera publiée au Journal officiel de la République française.

La Présidente

Isabelle FALQUE-PIERROTIN

**Nature de la délibération:** AUTORISATION UNIQUE