

Date de publication sur legifrance: 12/09/2013

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

**DELIBERATION n°2013-212 du 11 juillet 2013**

**Délibération n° 2013- 212 du 11 juillet 2013 concernant les traitements automatisés de données à caractère personnel relatifs à la passation, la gestion et l'exécution des contrats mis en oeuvre par les organismes d'assurances, de capitalisation, de réassurance, d'assistance et par leurs intermédiaires (norme simplifiée n°16).**

La Commission Nationale de l'Informatique et des Libertés,

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 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 de données à caractère personnel et à la libre circulation de ces données,

Vu le code de la mutualité,

Vu le code de la sécurité sociale,

Vu le code civil,

Vu le code de la santé publique,

Vu le code des postes et des communications électroniques,

Vu le code rural,

Vu le code monétaire et financier,

Vu le code général des impôts,

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés notamment son article 24,

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 modifiée relative à l'informatique, aux fichiers et aux libertés,

Vu le Code des assurances,

Vu la délibération n° 81-004 du 20 janvier 1981 concernant les traitements automatisés d'informations nominatives relatifs à la passation, la gestion et l'exécution des contrats mis en oeuvre par les organismes d'assurances, de capitalisation, de réassurances et d'assistance et par leurs intermédiaires ;

Après avoir entendu Monsieur Jean Paul AMOUDRY commissaire, en son rapport, et Monsieur

Jean-Alexandre SILVY commissaire du Gouvernement, en ses observations,

La délibération n° 81-004 du 20 janvier 1981 (norme simplifiée n°16) concernant les traitements automatisés d'informations nominatives relatifs à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurances, de capitalisation, de réassurances et d'assistance et par leurs intermédiaires, est devenue obsolète.

En vertu de l'article 24 de la loi du 6 janvier 1978 modifiée, la Commission nationale de l'informatique et des libertés est habilitée à établir des normes destinées à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

La présente norme permet aux responsables de traitement d'effectuer une déclaration simplifiée, dans les conditions qu'elle précise, pour les traitements relatifs à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurances.

Décide :

#### Article 1 : Champ d'application

Peut bénéficier de la procédure de la déclaration simplifiée de conformité à la présente norme tout traitement automatisé relatif à la passation, la gestion et l'exécution des contrats mis en œuvre par les organismes d'assurances, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurance.

Pour pouvoir faire l'objet de la procédure de déclaration simplifiée, ces traitements ne doivent pas donner lieu à des cessions, locations, interconnexions ou échanges autres que ceux nécessaires à l'accomplissement des fonctions énoncées à l'article 2. Ils doivent en outre satisfaire aux conditions énoncées aux articles qui suivent.

#### Article 2 : Finalités du traitement

Le traitement peut avoir tout ou partie des finalités suivantes:

- la passation et la gestion des contrats d'assurance, de capitalisation, de réassurance, et d'assistance (ci-après désignés par le « contrat ») avec :

l'étude des besoins spécifiques de chaque demandeur afin de proposer des contrats adaptés ;

l'examen, l'acceptation, le contrôle et la surveillance du risque ;

la gestion des contrats de la phase pré contractuelle à la résiliation du contrat ;

- l'exécution des contrats : les opérations techniques nécessaires à la mise en œuvre des garanties et des prestations ;
- l'élaboration des statistiques et études actuarielles ;
- l'exercice des recours et la gestion des réclamations et des contentieux ;
- 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 Informatique et Libertés.

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

Dès lors que les dispositions de l'article 32 de la loi n° 78.17 du 6 janvier 1978 modifiée ont été respectées lors du recueil des données à caractère personnel traitées, celles-ci doivent relever seulement des catégories suivantes, pour autant qu'elles soient nécessaires au respect des finalités du traitement :

- Les données relatives à l'identification des personnes parties, intéressées ou intervenantes au contrat : état civil ainsi que les pièces justifiant l'identité, les coordonnées et la nationalité ;
- Les données relatives à la situation familiale, économique, patrimoniale et financière ;
- Les données relatives à la situation professionnelle ;
- Les données nécessaires à l'appréciation du risque ;
- Les données nécessaires à la passation, l'application du contrat, et à la gestion des sinistres et des prestations ;
- Les informations relatives à la détermination ou à l'évaluation des préjudices ;
- Les données de localisation des personnes ou des biens en relation avec les risques assurés ;
- Les données relatives à la vie personnelle et aux habitudes de vie en relation avec les risques assurés ;
- Les données relatives à la santé lors de la souscription du contrat, sous réserve de l'obtention du consentement exprès de la personne concernée. Pour la mise en œuvre des garanties, le consentement de la personne est exigé sauf s'il ne peut être matériellement ou juridiquement recueilli, ou que l'organisme est soumis à une obligation légale de recueillir ces informations.

### Article 4 : Durées de conservation

En cas de conclusion d'un contrat, les données personnelles communiquées par les personnes intéressées, sont conservées par le responsable de traitement conformément à la durée nécessaire à l'exécution du contrat. Ces données sont ensuite archivées pour une durée prévue par les articles L.114-1 et suivants du code des assurances, l'article L.932-13 du code de la sécurité sociale et les dispositions du code civil relatives à la prescription.

En l'absence de conclusion d'un contrat, les données de santé peuvent être conservées par le responsable de traitement pendant une durée de deux ans en archive courante et trois ans en archive intermédiaire à des fins probatoires. S'agissant des autres données, elles peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (demande de renseignements ou de documentation, par exemple).

Concernant les données relatives aux cartes bancaires :

Les données relatives aux cartes bancaires doivent être supprimées une fois la transaction réalisée, c'est-à-dire dès son paiement effectif. Dans le cas d'un paiement par carte bancaire, elles peuvent être conservées pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, pour la durée prévue par l'article L. 133-24 du code monétaire et financier, en l'occurrence 13 mois suivant la date de débit. Ce délai peut être étendu à quinze mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé.

Ces données peuvent être conservées plus longtemps sous réserve d'obtenir le consentement exprès du client, préalablement informé de l'objectif poursuivi (faciliter le paiement des clients réguliers, par exemple). Ce consentement peut être recueilli par l'intermédiaire d'une case à cocher (non précochée par défaut), par exemple et ne peut résulter de l'acceptation de conditions générales.

Les données relatives au cryptogramme visuel ne doivent pas être stockées.

Lorsque la date d'expiration de la carte bancaire est atteinte, les données relatives à celles-ci doivent être supprimées.

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

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 qu'il collecte 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
- du transfert éventuel des données personnelles à destination d'un Etat non membre de l'Union Européenne

Lorsque le responsable de traitement utilise un service de communication au public en ligne (site internet), l'information relative à la finalité et aux droits des personnes peut être présente dans les courriers électroniques envoyés, sur la page d'accueil du site, et dans ses conditions générales d'utilisation par exemple.

Concernant l'exercice du droit d'opposition à l'analyse de sa navigation, l'outil permettant de désactiver la traçabilité mise en œuvre par l'outil d'analyse de fréquentation doit remplir les conditions suivantes :

un accès et une installation aisés pour tous les internautes sur l'ensemble des terminaux, des systèmes d'exploitation et des navigateurs internet ;

aucune information relative aux internautes ayant décidé d'exercer leur droit d'opposition ne doit être transmise à l'éditeur de l'outil d'analyse de fréquentation.

Par ailleurs, tout abonné ou 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 dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement;

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 qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

## Article 7 : Appréciation du risque

L'appréciation du risque comprend l'examen et l'évaluation des caractéristiques du risque pour en déterminer en particulier la fréquence, son coût moyen, le coût du sinistre maximum possible, en établir la tarification et en vérifier l'assurabilité. Les conditions d'acceptation et les conditions tarifaires sont fixées dans le cadre de la politique d'acceptation des risques établie conformément au

code des assurances à partir notamment de critères actuariels.

Aucune décision refusant un contrat à une personne ne pourra avoir pour seul fondement un traitement automatisé de données à caractère personnel, les personnes concernées devront être mises en mesure de présenter leurs observations.

#### Article 8 : 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...).

Dans le cas de l'utilisation d'un service de communication au public en ligne, le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à les rendre incompréhensibles à toute personne non autorisée à y avoir accès.

S'agissant des données de santé, le responsable de traitement s'engage à respecter les dispositions prévues par la 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.

#### Article 9 : Transferts de données vers l'étranger

Certains transferts de données à caractère personnel peuvent être réalisés vers des pays tiers à l'Union européenne, qui ne sont pas membres de l'Espace économique européen et qui n'ont pas été reconnus par une décision de la Commission européenne comme assurant un niveau de protection adéquat, dès lors que :

- 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 émises par la Commission européenne ou par l'adoption de règles internes d'entreprise ayant fait l'objet d'une décision favorable de la Commission nationale de l'informatique et des libertés ;
- le responsable de traitement a clairement informé les personnes de l'existence d'un transfert de données vers des pays tiers, et ce conformément aux dispositions de l'article 32 de la loi « Informatique et Libertés »;
- 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 oeuvre pour encadrer ce transfert.

- Conformément à l'article 69 de la loi du 6 janvier 1978 :
- Ces transferts sont réalisés dans le cadre de l'exécution des contrats (article 69, 5°, 6°) ou de la sauvegarde de la vie humaine pour la mise en oeuvre des garanties d'assistance (article 69, 1°)
- Ils sont également réalisés 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°).

Article 10 : L'utilisation d'un service de communication au public (site Internet)

Pour réaliser les finalités définies à l'article 2 la présente norme s'applique également dans le cas où le responsable de traitement utilise un service de communication au public en ligne.

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

Article 11 : Dispositions complémentaires

Les traitements de données à caractère personnel dont la mise en oeuvre est régulièrement intervenue avant la publication de la présente délibération sont réputés conformes, dès lors qu'ils auront été régulièrement mis en oeuvre et que leurs caractéristiques n'auront pas été modifiées.

Les traitements dont les finalités sont celles définies à l'article ci-dessus, qui comportent l'enregistrement d'informations n'appartenant pas aux catégories énumérées à l'article 3 ou aboutissant à la transmission d'informations à des destinataires autres que ceux définis à l'article 5 doivent faire l'objet de demandes de déclarations complémentaires.

Article 12

Les organismes d'assurances, de capitalisation, de réassurance, d'assistance et les intermédiaires d'assurance ayant effectué une déclaration simplifiée en référence à la norme simplifiée n°16 et qui ne respectent pas les conditions fixées par la présente norme, disposent d'un délai de douze mois à compter de la publication de la présente délibération pour mettre en conformité leur traitement.

La délibération n° 81-004 du 20 janvier 1981 concernant les traitements automatisés d'informations nominatives relatifs à la passation, la gestion et l'exécution des contrats mis en oeuvre par les organismes d'assurances, de capitalisation, de réassurances et d'assistance et par leurs intermédiaires, est abrogée.

Article 13

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

La Présidente

Isabelle FALQUE-PIERROTIN

**Nature de la délibération:** Norme simplifiée