

Date de publication sur legifrance: 26/02/2014

Commission Nationale de l'Informatique et des Libertés

DELIBERATION n°2014-014 du 23 janvier 2014

Délibération n° 2014-014 du 23 janvier 2014 portant création d'une autorisation unique concernant les traitements de données à caractère personnel relatifs à la consultation du Répertoire National d'Identification des Personnes Physiques (RNIPP) et à l'utilisation du numéro d'inscription au répertoire (NIR) mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance, les intermédiaires d'assurance et par l'AGIRA.

AU-031

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 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 25-1-6° 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 et les intermédiaires d'assurance sont fondés à utiliser le NIR pour les activités d'assurance maladie complémentaire, de maternité, d'invalidité, et de vieillesse lorsqu'ils interviennent en complément des régimes sociaux de base ou dans le cadre des relations avec les professionnels de santé, ou encore, pour l'indemnisation des accidents et pour la gestion des rentes.

La loi du 17 décembre 2007 permet la recherche des bénéficiaires des contrats d'assurance sur la vie non réclamés. A cet égard, la délibération n°2008-579 du 18 décembre 2008, autorise l'Association pour la gestion des informations sur le risque en assurance (AGIRA) à traiter les données à caractère personnel relatives aux décès transmises par l'INSEE pour le compte des organismes d'assurance, dans le cadre des traitements mis en œuvre aux fins de recherche des assurés et des bénéficiaires de contrats d'assurance sur la vie décédés. Le système permet ainsi aux organismes d'assurance membres de l'AGIRA, d'interroger le responsable de traitement (AGIRA), pour consulter le fichier.

Ces traitements relèvent du 6° 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 du II de l'article 25 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.

Décide :

D'adopter une autorisation unique pour les traitements automatisés ou non de données à caractère personnel relevant de l'article 25-1-6° ;

Les organismes mentionnés ci-dessous qui souhaiteront se référer à la présente autorisation unique adresseront 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 finalité la passation, la gestion et l'exécution des contrats d'assurance, de capitalisation, de réassurance, et d'assistance nécessitant :

- la collecte et le traitement du numéro d'inscription au répertoire (NIR) par les responsables de traitement dans les seuls cas suivants, à l'exclusion de toute utilisation aux fins d'identification des doublons ou des homonymies :
- pour leurs activités d'assurance maladie, maternité, invalidité, retraite supplémentaire en vertu des dispositions de l'article R.115-2-2° du code de la sécurité sociale ;

- pour leurs activités d'assurance pour les garanties pertes d'exploitation et perte d'emploi uniquement à des fins probatoires ;
- pour les relations avec les professionnels, les établissements et les institutions de santé en vertu des dispositions de l'article R.115-2-3° du code de la sécurité sociale ;
- pour les déclarations sociales des entreprises souscriptrices de contrats d'assurance en vertu de l'article R-115-2-6° du code de la sécurité sociale ;
- pour l'indemnisation des accidents, en vertu des dispositions des articles L.376-1 et L.454-1 du code de la sécurité sociale et plus spécifiquement dans le cadre des accidents de la circulation, en vertu des articles R 211-37 et R 211-38 du code des assurances ;
- pour la gestion des rentes, en vertu des dispositions de l'article 39A de l'annexe III du CGI et L.81 A du livre des procédures fiscales ;
- pour l'exécution des dispositions légales, réglementaires et administratives en vigueur.
- l'accès aux données du Registre National d'Identification des Personnes Physiques (RNIPP) :
- Les traitements mis en œuvre par l'AGIRA ont pour objet :
- la tenue d'une base de données relative aux personnes dont le décès est connu de l'INSEE, mise à jour mensuellement,
- la mise en place d'une plate-forme sécurisée permettant l'interrogation de cette base par les seuls organismes d'assurance qui interviennent dans le secteur de l'assurance sur la vie.
- Les traitements mis en œuvre par les organismes d'assurance ayant pour finalité exclusive la recherche tant des assurés que des bénéficiaires de contrats d'assurance sur la vie qui seraient décédés. Sont également visés par la présente autorisation les traitements visant à assurer la journalisation des requêtes et à réaliser des analyses statistiques sur l'interrogation de la base de données.

Les organismes d'assurance pourront consulter la base de données selon deux modalités :

- par voie d'interrogation ponctuelle sur un assuré ou un bénéficiaire ;
- par voie d'interrogations groupées, par l'envoi de fichiers portant sur tout ou partie de leurs assurés ou bénéficiaires ; ces interrogations groupées pourront porter sur la totalité de la base ou sur les seuls signalements de décès reçus durant la dernière année.

Toute interrogation doit indiquer au minimum les nom, prénom, date de naissance et sexe de la personne recherchée.

Les organismes susvisés à l'article 1er s'engagent à ne pas utiliser les données figurant sur la base AGIRA à d'autres fins que celles prévues par la loi du 17 décembre 2007.

Article 3 : Catégories de données à caractère personnel traitées

Peuvent être collectés, dans le cadre des finalités décrites à l'article 2 :

- le Numéro d'inscription au répertoire National d'Identification des Personnes Physiques (NIR) des personnes parties ou intéressées au contrat ;
- les données contenues dans la base de données tenue par l'AGIRA (et issues du RNIPP) aux fins de recherche des assurés et des bénéficiaires de contrats d'assurance sur la vie décédés, à savoir les seuls :
- nom patronymique, prénoms ;
- sexe ;
- date et lieu de naissance ;
- date et lieu du décès ;
- numéro d'acte de décès.

Article 4 : Durées de conservation des données

Le NIR de la personne concernée et les données du RNIPP accessibles par l'intermédiaire de l'Agira sont conservés par le responsable de traitement pour la durée nécessaire pour l'exécution du contrat dans les cas visés à l'article 2.

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.

Le fichier AGIRA est mis à jour chaque mois sur la base des éléments transmis par l'INSEE.

Les données communiquées aux organismes visés à l'article 1er et relatives aux assurés et aux bénéficiaires d'un contrat d'assurance sur la vie sont conservées dans les traitements de gestion conformément à la durée nécessaire à l'exécution du contrat.

Ces données sont ensuite archivées pour une durée qui correspond à la prescription légale.

Les données personnelles enregistrées sont supprimées lorsqu'il apparaît avec certitude au gestionnaire d'un dossier d'assurance sur la vie qu'elles se rapportent à un homonyme de l'assuré ou d'un bénéficiaire du contrat.

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, y compris dans le cadre d'un réseau de soins ;
- les sous traitants, les entités du même groupe 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 ;
- s'il y a lieu, les co-assureurs et réassureurs ainsi que les organismes professionnels et les fonds de garanties ;
- Les personnes intervenant au contrat ou dans l'instruction des dossiers tels que les avocats, experts, et officiers ministériels , enquêteurs, médecins et autres professionnels de santé 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 de sécurité sociale (assurances maladie, maternité, invalidité, décès, assurance retraite supplémentaire) ;
- les organismes et associations pratiquant la prévention, l'action sociale ou la gestion de réalisations sanitaires et sociales ;

b- en qualité de personnes intéressées au contrat :

- les souscripteurs, les assurés, les adhérents et les bénéficiaires des contrats ou les tiers

victimes et s'il y a lieu leurs ayants droit et représentants ;
c- en qualité de personnes habilitées au titre des tiers autorisés :

- s'il y a lieu les juridictions concernées, les arbitres, les médiateurs ;
- les 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.

Dans le cadre des données relatives aux personnes décédées, les personnes habilitées à recevoir communication de ces données sont :

- au sein des services de l'AGIRA, les gestionnaires habilités chargés de l'exploitation des fichiers de réponses issus des interrogations par lots ;
- au sein des organismes d'assurance, des institutions de prévoyance et leurs unions, et des mutuelles et leurs unions, les interrogations ponctuelles de la base de l'AGIRA ne peuvent être effectuées que par un nombre de gestionnaires habilités limité et adapté à la taille du portefeuille, disposant de certificats individuels et ayant vérifié la motivation des demandes d'interrogation. Les données issues des interrogations de la base de l'AGIRA sont utilisées par les personnels habilités à intervenir dans la gestion des contrats d'assurance sur la vie.

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...).

Les accès individuels à la base AGIRA s'effectuent après authentification mutuelle du système hébergeant le traitement et de l'utilisateur 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.

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

La délibération n°2008-579 du 18 décembre 2008, concernant les traitements mis en œuvre aux fins de recherche des assurés et des bénéficiaires de contrats d'assurance sur la vie décédés, portant sur les données à caractère personnel relatives aux décès transmises par l'INSEE, et réalisés par l'Association pour la gestion des informations sur le risque en assurance (AGIRA) pour le compte des organismes d'assurance, est abrogée.

Les responsables de traitements de données à caractère personnel visés à l'article 2 disposent d'un délai de 18 mois à compter de la publication de la présente délibération pour mettre en œuvre leurs traitements en conformité, en procédant soit à un engagement de conformité de la présente autorisation unique, soit à une demande d'autorisation précisant les différences entre le traitement envisagé et la présente autorisation unique.

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

La Présidente

Isabelle FALQUE-PIERROTIN

Nature de la délibération: AUTORISATION UNIQUE