Date de publication sur legifrance: 27/02/2018

Commission Nationale de l'Informatique et des Libertés

Décision n° MED-2018-006 du 8 février 2018
Décision n° MED-2018-006 du 8 février 2018 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés

La Présidente de 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 pénal ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 45 ;

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 ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2016-186C du 20 juin 2016 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tous traitements relatifs au Système national d'information interrégimes de l'assurance maladie (SNIIRAM) ;

Vu les procès-verbaux de contrôle n° 2016-186/1 du 14 septembre 2016, n° 2016-186/2 du 15 septembre 2016, n° 2016-186/3 du 28 septembre 2016, n° 2016-186/4 du 29 septembre 2016, n° 2016-186/5 du 9 novembre 2016, n° 2016-186/6 du 10 novembre 2016, n° 2016-186/7 du 8 mars 2017 et n° 2016-186/8 du 9 mars 2017 ;

Vu les autres pièces du dossier ;

L'historique de la procédure

Le 21 avril 2016, la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission), après avoir pris connaissance du projet de rapport de la Cour des comptes portant sur les données à caractère personnel gérées par l'Assurance Maladie relevant une sécurité insuffisante des données traitées, rendu public le 3 mai 2016, a retenu au nombre des thématiques de son programme annuel de contrôles le Système National d'Information Interrégimes de l'Assurance Maladie (ci-après SNIIRAM).

Le SNIIRAM a été créé par la loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale.

Aux termes de l'article L161-28-1 du code de la sécurité sociale, il contribue :

1° à la connaissance des dépenses de l'ensemble des régimes d'assurance maladie par circonscription géographique, par catégorie de professionnels responsables de ces dépenses et par professionnel ou établissement ;
2° à la transmission en retour aux prestataires de soins d'informations pertinentes relatives à leur activité et à leur recette, et s'il y a lieu à leurs prescriptions ;
3° à la définition, à la mise en œuvre et à l'évaluation des politiques de santé publique ;
4° à la constitution du système national des données de santé (…). Il est alimenté par les organismes gérant un régime de base d'assurance maladie.

Le traitement est mis en œuvre dans les conditions prévues à l'arrêté du 19 juillet 2013, pris après avis de la CNIL, modifié par l'arrêté du 6 octobre 2016. L'article 2 précise ainsi que les traitements mis en œuvre dans le cadre du SNIIRAM répondent à quatre finalités : l'amélioration de la qualité des soins, la meilleure gestion de l'assurance maladie, la meilleure gestion des politiques de santé et la transmission aux prestataires de soins des informations pertinentes relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions.

L'article 3 dresse la liste des données traitées qui comprend notamment des données relatives à l'assuré et au bénéficiaire des remboursements (sexe, année et mois de naissance, département et commune de résidence et, le cas échéant, date de décès), les informations relatives aux prestations fournies (nature détaillée des actes, dates de soins et de remboursement, mode de prise en charge, informations relatives au parcours de soin et à l'identification du professionnel) ainsi que des informations relatives à l'activité des établissements de santé.

L'article 5 dispose, quant à lui, que la gestion technique [de la base de données nationale] est confiée à la Caisse nationale de l'assurance maladie des travailleurs salariés (ci-après CNAMTS).

En application de la décision n° 2016-186C du 20 juin 2016 de la Présidente de la CNIL, des missions de contrôle sur place ont été diligentées entre les mois de septembre 2016 et mars 2017 afin de vérifier la conformité du SNIIRAM à la loi du 6 janvier 1978 modifiée (ci-après Loi Informatique et Libertés).

Les missions de vérification ont conduit les délégations de contrôle à se déplacer au sein des locaux de la CNAMTS à Paris, du centre d'hébergement de données d'Évreux, de la société SOPRA STERIA – prestataire chargé d'assurer la maintenance évolutive et corrective du SNIIRAM – et de la Caisse primaire d'assurance maladie (CPAM) de Loire-Atlantique. Des éléments ont par ailleurs été transmis par la CNAMTS le 29 juillet 2016 en réponse à un questionnaire adressé par la CNIL le 11 juillet de la même année dans le cadre d'un contrôle sur pièces (cf. point 1. de l'annexe de la mise en demeure détaillant les constats et informations obtenues).

La CNAMTS, au vu des éléments en possession de la CNIL, est considérée comme responsable de traitement de la base nationale SNIIRAM dans la mesure où, en plus d'assurer la gestion technique de la base conformément à l'article 5 de l'arrêté du 19 juillet 2013, elle est, comme elle l'indique elle-même, responsable du respect des règles de protection des données (au sens de la directive 95/46/CE) mais également (…) avec une grande marge d'autonomie, du fonctionnement opérationnel de la base (dont l'accomplissement des formalités CNIL) .

Elle a, par ailleurs, fourni la liste des personnes habilitées à accéder à tout ou partie du SNIIRAM. Il s'agit notamment des caisses nationales des régimes d'assurance maladie, des directions régionales du service médical, des directeurs coordinateurs de la gestion du risque du régime général, des médecins des agences régionales de santé, de Santé publique France, de la Haute Autorité de Santé, de l'Agence nationale de sécurité du médicament et des produits de santé, des ministères de la santé, de l'agriculture et de l'économie et des finances, de l'institut national des données de santé ainsi que des organismes de recherche tels que le centre national de la recherche scientifique ou l'institut national de la santé et de la recherche médicale.

Les manquements au regard des dispositions de la loi du 6 janvier 1978 modifiée

Les réponses de la CNAMTS au questionnaire de la CNIL ainsi que les missions de vérification effectuées les 14, 15, 28 et 29 septembre dans les locaux de la CNAMTS à Evreux, les 9 et 10 novembre 2016 dans ses locaux à Paris, le 8 mars 2017 auprès de la société SOPRA STERIA puis le 9 mars 2017 au sein de la CPAM de Loire-Atlantique ont mis en lumière de nombreux manquements à la sécurité des données à caractère personnel traitées dans le cadre du SNIIRAM.

Les multiples insuffisances en termes de sécurité concernent, notamment, la pseudonymisation des données, les procédures de sauvegarde, l'accès aux données par les utilisateurs du SNIIRAM et par des prestataires, la sécurité des postes de travail des utilisateurs du SNIIRAM, les extractions de données individuelles du SNIIRAM ainsi que la mise à disposition d'extractions de données agrégées du SNIIRAM aux partenaires (cf. annexe).

L'ensemble de ces faits constituent un manquement à l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée disposant que le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient

accès.

Il est en outre rappelé qu'en application des articles 226-17 et 226-24 du code pénal combinés, le fait pour une personne morale de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est notamment puni d'une peine d'amende pouvant atteindre 1.500.000 €.

En conséquence, la CNAMTS, sise 50 avenue du Professeur André Lemierre – 75020 Paris est mise en demeure, sous un délai de trois mois (3 mois) à compter de la notification de la présente décision et sous réserve des mesures qu'elle aurait déjà pu adopter, de :

- **prendre toute mesure pour garantir la sécurité et la confidentialité des données à caractère personnel traitées et en particulier, celles visées en annexe de la présente mise en demeure ;**
- **justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.**

À l'issue de ce délai, si la CNAMTS s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si la CNAMTS ne s'est pas conformée à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente

Isabelle FALQUE-PIERROTIN