Délibération n° 2021-172 du 21 juillet 2021

de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Consultation des remboursements maladies pour les bénéficiaires SPME* »

exploité par le Service des Prestations Médicales de l'Etat (SPME)

présenté par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

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 et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° n° 486 du 17 juillet 1948 relative à l'octroi des allocations pour charges de famille, des prestations médicales, chirurgicales et pharmaceutiques aux fonctionnaires de l'Etat et de la Commune ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 231 du 3 octobre 2005 portant création d'un Service des Prestations Médicales de l'Etat ;

Vu l'Ordonnance Souveraine n° 2011-3413 du 29 aout 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré ;

Vu la demande d'avis présentée le 29 avril 2021 par le Ministre d'Etat, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité *« Consultation des remboursements maladies pour les bénéficiaires SPME* » du Service des Prestations Médicales de l'Etat ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 25 juin 2021, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 21 juillet 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

L'Ordonnance Souveraine n° 231 du 3 octobre 2005 portant création d'un Service des Prestations Médicales de l'Etat (SPME) dispose que ce dernier est chargé « *de gérer les prestations accordées par l'Etat au titre (…) des prestations familiales et autres avantages sociaux y afférents* ».

Le SPME souhaite désormais permettre à ses bénéficiaires de consulter leurs remboursements en ligne grâce à une application web accessible depuis ordinateurs et smartphones.

Aussi, le Ministre d'Etat souhaite soumettre à l'avis de la Commission, conformément aux dispositions de l'article 7 de la Loi n° 1.165 du 23 décembre 1993, le traitement ayant pour finalité « *Consultation des remboursements maladies pour les bénéficiaires SPME* ».

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité la « *Consultation des remboursements maladies pour les bénéficiaires SPME* ».

Le responsable de traitement précise qu'il concerne les bénéficiaires SPME, à savoir les assurés et leurs ayants-droit, mais également les professionnels de santé et les fonctionnaires et agents du SPME en charge du traitement.

Les fonctionnalités ouvertes aux bénéficiaires SPME sont :

- Consulter les remboursements par bénéficiaire et/ou praticien ;
- Télécharger le fichier PDF du détail du remboursement ;
- Transmettre les données de remboursement à son assurance maladie complémentaire ;
- Exercice du droit d'accès.

La Commission constate également que le traitement permet d'afficher la carte d'assuré dématérialisée du bénéficiaire et les cartes de feuilles de soins électroniques des ayants-droit, et de notifier (par mail ou notification de l'application mobile) ce dernier de l'arrivée de nouveaux remboursements, qu'il lui appartient de consulter sur le téléservice.

Elle constate de plus que la carte FSE (Feuille de Soins Electronique) peut être utilisée par une personne dite de confiance, par l'application mobile.

Les fonctionnaires et agents du SPME disposent des fonctionnalités suivantes :

- Générer le courrier contenant les codes d'activation des comptes personnels ;

- Ajout d'une assurance mutuelle complémentaire ;
- Réponses aux demandes de droit d'accès.

La Commission considère que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

Le traitement est justifié par le respect d'une obligation légale, le consentement des personnes concernées et la réalisation d'un intérêt légitime, sans que ne soient méconnus les droits et libertés fondamentaux des personnes concernées.

L'Ordonnance Souveraine n° 231 du 3 octobre 2005 portant création d'un Service des Prestations Médicales de l'Etat (SPME) dispose que ce dernier est chargé « *de gérer les prestations accordées par l'Etat au titre (…) des prestations familiales et autres avantages sociaux y afférents* ».

La Commission rappelle également que les modalités de remboursement des prestations médicales, chirurgicales et pharmaceutiques sont précisées par différents textes visés notamment dans sa délibération n° 2013-26 du 6 mars 2013 portant avis favorable sur la demande présentée par le Ministre d'Etat relative à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Décomptes – gestion et remboursement des prestations médicales en nature* », dénommé « *décompte des prestations médicales en nature* », du Service des Prestations Médicales de l'Etat.

En outre, il précise que le consentement des personnes concernées est formalisé par un acte positif clair matérialisé par le biais d'une case à cocher mentionnant « *J'accepte que mes données personnelles soient traitées dans le cadre du téléservice « consulter en ligne ses remboursements médicaux effectués par le SPME »* », ainsi que par l'acceptation préalable des conditions générales d'utilisation du téléservice, indispensable pour la création du compte sécurisé et pour l'accès à la démarche en ligne.

Par ailleurs, l'intérêt légitime trouve son fondement dans la volonté de l'Administration de simplifier les démarches administratives des administrés en leur permettant de consulter leurs remboursements sans envoi par courrier, ce qui s'inscrit dans le cadre de l'Ordonnance Souveraine n° 2011-3413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré et contribue à la démarche écologique de la Principauté.

La Commission rappelle que conformément aux dispositions de l'article 43 de l'Ordonnance Souveraine susvisée *« (…) la création d'un téléservice ne saurait toutefois avoir pour effet de supprimer la possibilité pour l'usager, d'accomplir les démarches, formalités ou paiements qui en sont l'objet par des voies autres qu'électroniques* ».

Aussi, la Commission considère que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Le responsable de traitement exploite les informations dites « *sensibles* » protégées par l'article 12 de la Loi n° 1.165 suivantes :

- Données de santé : nom et prénom du praticien et professionnel de santé ayant prescrit ou réalisé des actes, taux de prise en charge général selon les personnes assurées, libellé général de l'acte (sans référence à la nomenclature des actes), taux de prise en charge de chaque acte, exonération du ticket modérateur.

La licéité de la collecte a déjà été analysée par la Commission dans sa délibération n° 2013-26 du 6 mars 2013 relative au traitement ayant pour finalité « *Décomptes, gestion et remboursement des prestations médicales en nature* », le présent téléservice n'étant qu'une modalité d'accès offerte aux bénéficiaires à leurs remboursements effectués par le traitement métier du SPME.

Les informations nominatives également traitées sont :

- Identité, situation de famille : titre, matricule, nom, nom marital, prénoms de l'assuré et de ses ayants-droits, date de naissance, nationalité, situation familiale (lien familial entre les assurés distinguant le bénéficiaire de ses ayants-droit) ;
- adresses et coordonnées : adresse postale de l'assuré, adresse email de l'assuré ;
- données d'identification électronique : identifiant web ;
- informations temporelles : données d'horodatage, logs de connexion.

Les informations ont pour origine le traitement du SPME ayant pour finalité « *Décomptes gestion et remboursement des prestations médicales en nature* », exceptées celles temporelles qui sont générées par le module de la démarche en ligne.

La Commission considère que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

➢ *Sur l'information préalable des personnes concernées*

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée par le biais d'un courrier adressé à l'intéressé et d'une mention particulière intégrée dans un document d'ordre général accessible en ligne.

Ladite mention, jointe au dossier, est conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993. La Commission relève à cet égard que les CGU informent les personnes concernées que ce téléservice est facultatif et qu'elles peuvent revenir si elles le désirent à une solution d'envoi papier des décomptes.

➢ *Sur l'exercice du droit d'accès, de modification et de mise à jour*

Le responsable de traitement indique que le droit d'accès est exercé par un accès en ligne au dossier.

La Commission constate ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

V. Sur les destinataires et les personnes ayant accès au traitement

- ***Sur les destinataires***

La Commission constate que les informations peuvent être communiquées aux mutuelles des bénéficiaires du SPME, avec l'accord préalable des personnes concernées, par le biais d'un accès sécurisé.

Elle constate que cette communication est conforme aux exigences légales.

Par ailleurs elle prend acte des précisions selon lesquelles le module Google Analytics a été désactivé.

- ***Sur les accès au traitement***

Le responsable de traitement indique qu'ont accès au traitement :

- Les personnels du SPME habilités à la génération du code d'activation : tout droit d'inscription, modification et suppression ;
- Les administrateurs réseaux et systèmes d'information de la Direction des Systèmes d'Information (ou tiers agissant pour son compte ou sous son autorité) : accès en inscription, modification, mises à jour, à des fins d'administration et de maintenance, de suivi et développement, et de sécurité ;
- Les personnels de la Direction de l'administration Numérique ou tiers intervenant pour son compte ayant un rôle d'assistance à maîtrise d'ouvrage, dûment habilités : assistance à maitrise d'ouvrage, qui n'accède à aucune donnée métier du téléservice ;
- Les personnels habilités des Caisses Sociales de Monaco intervenant pour le compte du responsable de traitement : accès en inscription, modification, mises à jour, à des fins d'administration et de maintenance, de suivi et développement, et de sécurité.

La Commission rappelle qu'en cas de recours à des prestataires, leurs accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, conformément à l'article 17 de la Loi n° 1.165. De plus, ils sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement.

Elle relève par ailleurs que les bénéficiaires pourront accéder à leur propre compte.

La Commission considère que ces accès sont justifiés.

VI. Sur les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement fait l'objet d'interconnexions avec les traitements de l'Etat légalement mis en œuvre ayant pour finalités :

- « *Gestion des habilitations et des accès au Système d'information* » afin de disposer des éléments permettant aux agents de l'Etat de se connecter au réseau afin d'exécuter leurs missions selon leurs profils ;
- « *Gestion de la messagerie professionnelle* », afin de permettre aux acteurs du traitement de pouvoir échanger dans le cadre de leurs fonctions ;
- « *Gestion et analyse des évènements du système d'information* » à des fins de traçabilité et de sécurité ;

- « *Gestion du compte permettant aux usagers d'entreprendre des démarches par téléservices* », pour permettre aux usagers d'accéder au traitement via leurs comptes ;
- « *Décomptes, gestion et remboursement des prestations médicales en nature* », afin de pouvoir afficher les données de l'usager dans le téléservice ;
- « *Dématérialisation des demandes de remboursement de prestations médicales* » afin de pouvoir accéder aux demandes de remboursement dans le téléservice.

Il est également interconnecté avec le traitement légalement mis en œuvre par les Caisses Sociales de Monaco ayant pour finalité « *Gestion des accès au système d'information opérés par les Caisses Sociales* », permettant à ses agents de se connecter au réseau afin d'exécuter leurs missions selon leurs profils.

La Commission relève que ces interconnexions sont conformes aux exigences légales.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation.

Cependant les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

En outre, la Commission constate l'utilisation de reCAPTCHA Google qui implique un transfert d'informations vers les Etats-Unis et rappelle qu'il doit être mis fin à l'utilisation de cette solution.

Elle rappelle en effet que toute utilisation d'outils subordonnant l'accès à un service à un transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat doit disposer d'un fondement juridique apportant des garanties appropriées audit transfert.

Enfin, la Commission rappelle que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur la durée de conservation

Les données de santé sont conservées 18 mois sur le téléservice mais ne sont consultable que sur 13 mois glissants par les usagers.

En ce qui concerne les autres données, le responsable de traitement indique que les informations sont conservées « *13 mois après la désactivation du compte* » excepté les données d'identification électronique et les données de connexion qui sont effacées au bout d'un an.

Si la Commission estime que la durée de 13 mois après la désactivation du compte est conforme aux exigences légales, elle rappelle que celui-ci ne saurait étendre les durées de conservation du traitement métier qui ont été fixées « *à 5 ans à compter de la fin de l'année comptable au cours de laquelle le paiement ou refus de paiement aura été réalisé* »

(avant éventuel archivage à des fins statistiques ou historique) par délibération 2016-52 en date du 20 avril 2016 portant avis favorable à la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *dématérialisation des demandes de remboursement de prestations médicales*», *dénommé « F.S.E. : Feuilles de Soins Electroniques (application en mode Web)* » du Service des prestations médicales de l'Etat, présenté par le Ministre d'Etat.

Après en avoir délibéré, la Commission :

Rappelle que :

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé ;

- la durée de 13 mois après la désactivation du compte est conforme aux exigences légales, elle rappelle que celui-ci ne saurait étendre les durées de conservation du traitement métier qui ont été fixées « *à 5 ans à compter de la fin de l'année comptable au cours de laquelle le paiement ou refus de paiement aura été réalisé* » (avant éventuel archivage à des fins statistiques ou historique) par délibération n° 2016-52.

Acte que le délai pour le remplacement du Google ReCAPTCHA est échu et qu'il doit désormais être mis fin à l'utilisation de toute solution impliquant un transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat, en l'absence de fondement juridique apportant des garanties appropriées audit transfert.

A la condition de la prise en compte des éléments qui précèdent,

la Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre, par le Ministre d'Etat du traitement automatisé d'informations nominatives ayant pour finalité « *Consultation des remboursements maladies pour les bénéficiaires SPME* » du Service des Prestations Médicales de l'Etat.**

Le Président

Guy MAGNAN