

Délibération n° 2019-169 du 20 novembre 2019

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

« *Gestion du portail de e-Santé de la Principauté de Monaco* »

exploité par le Département des Affaires Sociales et de la Santé (DASS)

présenté par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention 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 du 28 janvier 1981 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 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° 5.641 du 14 décembre 2015 portant création d'une Direction de l'Action et de l'Aide Sociales ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la délibération n° 2019-083 du 15 mai 2019 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les modalités de dépôt et la durée de conservation des cookies et autres traceurs sur les terminaux d'utilisateurs de réseaux de communication électronique ;

Vu la demande d'avis déposée par le Ministre d'Etat le 11 septembre 2019 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion du portail de e-Santé de la Principauté de Monaco* » ;

Vu la prorogation du délai d'examen de ladite demande d'avis notifiée au représentant du responsable de traitement le 8 novembre 2019, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 20 novembre 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Afin de gérer un portefeuille de services numériques à destination des patients (usagers) et des professionnels de santé autorisés à exercer en Principauté, le Gouvernement Princier souhaite mettre en place un portail de e-Santé qui sera exploité par le Département des Affaires Sociales et de la Santé (DASS).

Le traitement automatisé d'informations nominatives objet de la présente délibération est donc soumis à l'avis de la Commission conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Ce traitement a pour finalité « *Gestion du portail de e-santé de la Principauté de Monaco* ».

Les personnes concernées sont les professionnels de santé autorisés à exercer à Monaco, les patients du professionnel de santé utilisant l'agenda, les patients utilisateurs du portail (MC et étrangers), les collaborateurs du DASS (médecins inspecteurs de la Direction de l'Action Sanitaire (DASA) et membres 'Administrateur'), les administrateurs systèmes et les visiteurs du site.

Enfin, les fonctionnalités sont les suivantes :

- gestion d'un annuaire en ligne de tous les professionnels de santé autorisés à exercer à Monaco ;
- gestion d'un service de prise de rendez-vous en ligne sur des créneaux spécifiques et déterminés par le professionnel de santé ;
- gestion d'un service d'actualités de santé à destination du grand public et des professionnels de santé ;
- gestion d'un forum d'échange avec modérateur entre les professionnels de santé uniquement et le Gouvernement de Monaco ;
- gestion des comptes utilisateurs (patients et professionnels de santé) ;
- gestion des habilitations (matrice des droits, gestion et création des profils, audit trail) ;
- établissement de statistiques (tableau de bord, reporting).

Concernant le forum d'échange, la Commission prend acte des précisions du responsable de traitement selon lesquelles ledit forum « *permettra aux professionnels de santé uniquement (pas aux patients ni aux visiteurs) d'interagir avec le Gouvernement de Monaco (utilisateurs ayant les droits d'Administration sur le portail) sur des sujets en lien avec le projet de e-Santé de la Principauté* ».

La Commission constate ainsi 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 tout d'abord justifié par le consentement de la ou des personne(s) concernée(s).

La Commission relève ainsi que le consentement des professionnels de santé « *aura été préalablement recueilli à la publication dans l'annuaire du portail des informations détaillées les concernant* » et que « *Pour les professionnels qui n'auraient pas donné leur consentement à la publication de ces informations, seuls les éléments figurant sur leur autorisation d'exercer (nom, prénom, adresse, activité) seront publiés dans l'annuaire du portail. Ceci faisant partie des missions de la DASA de rendre publiques ces informations* ».

Elle note également que les patients, quant à eux, « *doivent cocher la case d'acceptation des conditions générales d'utilisation du portail et avoir pris connaissance des informations relatives à la protection de leurs informations nominatives avant de valider la création de leur compte utilisateur* ».

Le responsable de traitement précise en outre que les patients « *sont également informés des modalités de dépôt des cookies et autres traceurs ainsi que de leur durée de conservation lors de leur première connexion au portail de santé* ».

Le traitement est par ailleurs justifié par un motif d'intérêt public.

A cet égard, la Commission constate que « *La mise en place du portail de e-Santé de la Principauté de Monaco est la volonté exprimée du Gouvernement de mettre à disposition de tous les usagers (professionnels de santé et patients) un service d'intérêt public au travers duquel les utilisateurs trouveront un moyen facilité d'accéder à tout ce qui concerne la santé sur Monaco* ».

Le responsable de traitement indique par ailleurs que « *L'objectif de ce portail est d'offrir un service d'excellence, d'améliorer la qualité de vie du patient et la qualité de travail du professionnel de santé* » et que « *Par ce biais, le Gouvernement Princier affirme sa stratégie de santé publique* ».

Le traitement est enfin justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission prend ainsi acte des précisions du responsable de traitement selon lesquelles « *Ce projet s'inscrit pleinement dans la mission du Département des Affaires Sociales et de la Santé (DASS) et de la Direction de l'Action Sanitaire (DASA)* » puisqu'en effet « *le DASS est en charge de conduire les politiques publiques ayant trait notamment au domaine de la santé publique* » et que la « *DASA contribue elle, à l'élaboration de la politique de santé publique, assure la planification de l'offre de soins au regard des besoins de la population et délivre les agréments et autorisations d'exercice aux professionnels de santé* ».

La Commission considère donc que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- données de santé du patient utilisateur : date et heure du rendez-vous du patient, motif de consultation choisi par le patient, commentaire libre du patient (à l'attention du professionnel de santé pour lequel le rendez-vous est pris), agenda du professionnel de santé (non visible par les utilisateurs du portail), contenu des messages de prérequis (consignes rédigées par le professionnel de santé) adressés aux patients avant la validation de leur rendez-vous, contenu de l'email de confirmation du rendez-vous avec le professionnel de santé (email envoyé au patient lors de la validation du rendez-vous et reprenant les informations du rendez-vous sélectionné : date, heure, motif de consultation, praticien consulté), contenu de l'email de rappel de rendez-vous avec le professionnel de santé (email envoyé au patient la veille du rendez-vous et reprenant les informations du rendez-vous sélectionné : date, heure, motif de consultation, praticien consulté), contenu de l'email d'information de libération d'un créneau disponible pour un motif de consultation sélectionné par le patient chez un professionnel de santé donné (email envoyé au patient lors de la libération d'un créneau correspondant aux choix du patient et reprenant les informations du motif et du praticien sélectionnés : date, heure, motif de consultation, praticien consulté), contenu du SMS de confirmation du rendez-vous avec le professionnel de santé (SMS de 160 caractères maximum envoyé au patient lors de la validation du rendez-vous et reprenant les informations du rendez-vous sélectionné : date, heure, motif de consultation, praticien consulté) ; contenu du SMS de rappel de rendez-vous avec le professionnel de santé (SMS de 160 caractères maximum envoyé au patient la veille du rendez-vous et reprenant les informations du rendez-vous sélectionné : date, heure, motif de consultation, praticien consulté), contenu du SMS de modification du rendez-vous avec le professionnel de santé (SMS de 160 caractères maximum envoyé au patient lors de toute modification du rendez-vous par le patient ou par le professionnel de santé et reprenant les informations du rendez-vous modifié : date, heure, motif de consultation, praticien consulté), contenu du SMS d'annulation du rendez-vous avec le professionnel de santé (SMS de 160 caractères maximum envoyé au patient en cas d'annulation du rendez-vous par le patient ou par le professionnel de santé et reprenant les informations du rendez-vous annulé : date, heure, motif de consultation, praticien consulté), notes, consignes entre le professionnel de santé et son secrétariat (systèmes de notes permettant d'envoyer un message via l'agenda, d'y associer un patient et un rendez-vous, d'y saisir ou visualiser des commentaires , avec affichage des messages reçus en temps réel et gestion des notes à traiter/traitées), contenu des pièces jointes liées à un patient (le professionnel de santé peut inclure des pièces jointes – ordonnances, comptes rendus – dans la fiche patient de son agenda), statistiques du patient (nombre de rendez-vous pris, honorés, annulés, compte-rendu de rendez-vous), articles sur la santé publiés dans le service Actualités du portail (articles rédigés, validés, publiés par les personnes habilitées du DASS et de la DASA) ;
- identité de l'utilisateur (professionnel de santé, patient, aidé, personnes habilitées) : civilité, genre (homme/femme), nom d'usage, nom de naissance, prénom, date de naissance, contenu de l'email de confirmation de l'inscription de l'utilisateur (reprend l'identité de l'utilisateur), langue préférée ;
- adresses et coordonnées : nom de l'établissement de santé, nom du cabinet privé, nom du laboratoire, nom de la pharmacie, nom des services de l'établissement de santé, adresse de l'établissement de santé, du cabinet privé, du laboratoire, de la pharmacie, informations d'accès à l'établissement de santé, au service au sein de l'établissement de santé, au cabinet privé, au laboratoire, à la pharmacie (interphone, ascenseur, accès handicapé, digicode, étage, bâtiment), horaires d'ouverture de l'établissement de santé, des services de l'établissement de santé, du cabinet privé, du laboratoire, de la pharmacie, numéro de téléphone portable (non diffusé sur le portail, utilisé pour l'OTP et la réception de SMS), numéro de téléphone de l'établissement de santé, des services de l'établissement de santé,

- du cabinet privé, du laboratoire, de la pharmacie, nom des parkings à proximité de l'établissement de santé, du cabinet privé, du laboratoire, de la pharmacie ;
- formation, diplômes, vie professionnelle : titre du professionnel de santé, présentation du professionnel de santé (texte libre rédigé par le professionnel de santé et validé par le DASS et la DASA avant publication), description (présentation) de l'établissement de santé et des services (texte libre rédigé par l'établissement de santé et validé par le DASS/DASA avant publication), photo du professionnel de santé, photo de l'établissement de santé, spécialités, sous-spécialités, expertises du professionnel de santé, secteur de convention du professionnel de santé (conventionné CCSS ou non), langues parlées par le professionnel de santé, moyens de paiement acceptés par le professionnel de santé (espèces, chèque, carte bancaire, tiers-payant, carte vitale), montant des honoraires du professionnel de santé, diplômes du professionnel de santé (intitulé, lieu et date d'obtention), lieu(x) de consultation du professionnel de santé (un ou plusieurs cabinet(s) privé(s) et/ou un ou plusieurs service(s) d'un établissement de santé), lien vers site internet du professionnel de santé (si ce dernier souhaite y faire référence), créneaux de consultation du professionnel de santé, motifs de consultation proposés par le service de l'établissement de santé, le professionnel de santé, le laboratoire, durée de consultation, délai minimum avant prise de rendez-vous, délai maximum avant prise de rendez-vous, motif de consultation réservable en ligne (oui/non), message du professionnel de santé dans le service Forum du portail sur une catégorie, sous-catégorie ou sujet de discussion (ne contenant aucune donnée de santé, ni aucune donnée nominative ; si un message comportant ce type de données figurait dans le forum, ce message serait supprimé par le modérateur) ;
- données d'identification électronique : adresse email (identifiant de connexion), mot de passe, mot de passe à usage unique (reçu par SMS automatique), adresse email de contact de l'établissement de santé, du cabinet privé, du laboratoire, de la pharmacie ;
- informations temporelles : date et heure de dernière connexion de l'utilisateur, date et heure du dernier message sur un sujet de discussion sur le Forum ;
- cookies de session (cookies techniques) : sngcookie, JSESSIONIDSSO, JSESSIONID, XSRF-TOKEN, IDSLANG, sourceUrl, _keldoc_session, CookieInformationConsent et nehs-security ;
- cookies de mesure d'audience : adresse IP (avec anonymisation des 2 derniers octets), pages visitées et leur nombre, nombre d'affichage par page, durée passée sur chaque page, nombre de clics, nom et version du navigateur web de l'internaute, système d'exploitation de l'utilisateur, horodatage d'accès, nombre et nom des documents téléchargés.

Concernant les moyens de paiement acceptés, la Commission prend acte des précisions du responsable de traitement selon lesquelles « *aucun règlement ne s'effectue via le portail en ligne* » et qu'il n'y a « *aucune récupération de données bancaires* ».

Les informations relatives aux données de santé du patient utilisateur, l'identité de l'utilisateur, les adresses et coordonnées ainsi que les données d'identification électronique ont pour origine l'utilisateur concerné (professionnels de santé via un fichier de recueil d'informations et les patients via le formulaire d'inscription du portail e-santé).

Les informations relatives à la formation, aux diplômes et à la vie professionnelle ont pour origine le professionnel de santé via un fichier de recueil d'informations.

Enfin, les informations temporelles ainsi que les cookies ont pour origine le portail e-Santé.

La Commission considère ainsi 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

L'information préalable des personnes concernées est effectuée par le biais d'une rubrique propre à la protection des données accessible en ligne et par le biais d'une mention particulière intégrée dans un document d'ordre général.

A l'analyse de ces documents, la Commission considère que ceux-ci sont conformes à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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

Le droit d'accès s'exerce par courrier électronique, par voie postale et par un accès en ligne à son dossier.

La Commission prend acte des précisions selon lesquelles le droit d'accès aux données de santé peut s'effectuer soit par le biais de la plateforme, soit auprès des professionnels de santé concernés.

S'agissant de l'exercice du droit d'accès par voie électronique, la Commission considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

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 personnes ayant accès au traitement

Les personnes habilitées à avoir accès au traitement sont :

- les professionnels de santé autorisés à exercer à Monaco : accès à leur propre compte uniquement ;
- les patients du professionnel de santé utilisant l'agenda : accès à leur propre compte uniquement ;
- les patients utilisateurs du portail (MC et étrangers) : accès à leur propre compte uniquement ;
- les collaborateurs du DASS (médecins inspecteurs de la DASA et membres 'Administrateur') : validation des données collectées auprès des professionnels de santé ;
- les administrateurs systèmes : accès aux sauvegardes (aucun accès aux données de santé).

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'un rapprochement avec un traitement ayant pour finalité « *Gestion des autorisations d'exercer des professionnels de santé* ».

Ce traitement n'ayant pas fait l'objet de formalité auprès de la CCIN, la Commission demande au responsable de traitement de le lui soumettre dans les plus brefs.

Le responsable de traitement indique par ailleurs que le présent traitement fait également l'objet d'une interconnexion avec le traitement ayant pour finalité « *Gestion de prise de rdv de l'établissement de santé* » dont les responsables de traitement sont les établissements de santé (CHPG, IM2S et CCTM).

Il fait également l'objet de rapprochements avec les traitements suivants :

- « *Gestion de prise de rdv de l'établissement de santé* » dont le responsable de traitement est le Centre d'Hémodialyse Privé de Monaco (CHPM) ;
- « *Gestion de prise de rdv du praticien libéral* » dont les responsables de traitement sont les professionnels de santé utilisateurs de la plateforme.

A cet égard la Commission rappelle que les rapprochements et interconnexions doivent être effectués avec des traitements légalement mis en œuvre.

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 particulière.

La Commission rappelle néanmoins que les comptes utilisateurs doivent être protégés par un mot de passe réputé fort.

Par ailleurs, elle rappelle que les comptes administrateurs doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

La Commission rappelle également 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 informations relatives aux données de santé du patient utilisateur, à l'identité de l'utilisateur, aux adresses et coordonnées de l'utilisateur ainsi que les données d'identification électronique sont conservées tant que le compte de l'utilisateur utilisant ces données est actif.

A cet égard le responsable de traitement précise que les données sont supprimées après une période d'inactivité de 3 ans puis un archivage intermédiaire de 5 ans.

Les informations relatives à la formation, aux diplômes et à la vie professionnelle sont conservées tant que le praticien accepte la diffusion d'informations détaillées le concernant ou tant qu'il dispose d'une autorisation d'exercer en Principauté.

Les informations temporelles sont conservées 12 mois maximum.

Les cookies de navigation sont conservés le temps de la session à l'exception de CookieInformationConsent qui est conservé 13 mois et de nehs-security qui est conservé 7200 s.

Enfin les cookies de mesure d'audience sont conservés 13 mois.

La Commission considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que :

- les rapprochements et interconnexions doivent être effectués avec des traitements légalement mis en œuvre ;
- les comptes utilisateurs doivent être protégés par un mot de passe réputé fort ;
- les comptes administrateurs doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Demande que le traitement ayant pour finalité « *Gestion des autorisations d'exercer des professions de santé* » lui soit soumis dans les plus brefs délais.

Sous le bénéfice de la prise en compte de ce qui précède,

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 « *Gestion du portail de e-Santé de la Principauté de Monaco* ».**

Le Président

Guy MAGNAN