

Délibération n° 2021-185 du 15 septembre 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

« *Gestion du site internet du CHPG* »

présenté par le Centre Hospitalier Princesse Grace

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° 127 du 15 janvier 1930 constituant l'hôpital en établissement public autonome ;

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

Vu l'Ordonnance Souveraine n° 5.095 du 14 février 1973 sur l'organisation et le fonctionnement du Centre Hospitalier Princesse Grace, 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 la délibération n° 2011-82 du 21 octobre 2011 portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par le Centre Hospitalier Princesse Grace, le 2 juin 2021, portant sur la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion du site internet du CHPG* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 30 juillet 2021, conformément à l'article 19 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 15 septembre 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Aux termes de la Loi n° 127 du 15 janvier 1930, le Centre Hospitalier Princesse Grace (CHPG) est un établissement public autonome.

Le traitement 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

Le responsable de traitement indique que le traitement a pour finalité « *Gestion du site internet du CHPG* ».

Les personnes concernées sont tous les publics.

Enfin, les fonctionnalités sont les suivantes :

- présentation des services de l'hôpital : activité, équipes de professionnels de santé, contact ;
- diffusion des règles de fonctionnement, d'hygiène, d'organisation de l'hôpital ;
- diffusion des informations sur l'actualité de l'établissement ;
- publication des avis de recrutement ;
- statistiques de connexion (utilisation de l'outil piwik (Matomo) sur deux octets) : nombre de visites, origine des connexions, nombre de pages consultées, mots clés utilisés sur les moteurs de recherche, temps de connexion ;
- service de paiement en ligne ;
- formulaire de contact ;
- gestion des candidatures (formulaire) ;
- gestion des demandes de stages (formulaire) ;
- lien avec les réseaux sociaux (Facebook, Twitter) ;
- accessibilité malvoyants.

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 responsable de traitement indique que le traitement est justifié par un motif d'intérêt public et 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.

A cet effet, il précise que « *Le CHPG est un établissement public autonome depuis la Loi n° 127 du 15 janvier 1930* » et qu' « *En son sein, l'activité médicale est répartie aux urgences et dans les services de consultation, de soins et d'hospitalisation* ».

La Commission relève par ailleurs que « *Son activité comporte également la gestion du CAP FLEURI, A QIETUDINE, CRIII, Monaco Princesse Grace Check-up Unit, l'établissement du don du sang, l'institut de formation* ».

Elle note également que « *L'information des personnes est essentielle à la réalisation de sa mission* ».

La Commission constate ainsi que le traitement dont s'agit « *permet de présenter les activités de l'établissement et d'informer toutes personnes intéressées (patient, résident et leur famille, visiteur, professionnel de santé, étudiant)* ».

Elle considère donc 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

Les informations nominatives traitées sont :

- identité :
 - o équipe médicale : nom et prénom, chef de service, adjoints, praticiens hospitaliers, assistant ;
 - o équipe paramédicale : cadre supérieur de santé, cadre de santé ;
 - o nom et prénom de la secrétaire ;
- adresses et coordonnées : numéro de téléphone et fax du secrétariat médical, email de contact du service, email du médecin ;
- formation, diplômes, vie professionnelle : titre (docteur, professeur,...), activité, CV du professionnel de santé ;
- paiement en ligne : numéro du titre, montant, état du paiement par carte bancaire ;
- formulaire de candidature : prénom, nom, email, poste visé, remarques, CV, lettre de motivation ;
- formulaire de demande de stage : nom, établissement extérieur, formation, discipline, période de stage, civilité, nom, prénom, adresse complète, téléphone fixe, téléphone mobile, email, date de naissance, lettre de motivation, CV.
- Formulaire de contact : prénom, nom, email, sujet, message ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux informations ;
- statistiques Piwik (Matomo) sur 2 octets : nombre de visite, origine des connexions, nombre de pages connectées, mots clés utilisés sur les moteurs de recherches, temps de connexion.

Les informations relatives à l'identité, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion des Ressources Humaines et paie* ».

Les informations relatives aux adresses et coordonnées ont pour origine le traitement ayant pour finalité « *Gestion des services de téléphonie* ».

Les informations relatives au paiement en ligne ont pour origine le patient.

Les informations contenues dans le formulaire de candidature ont pour origine le postulant.

Les informations contenues dans le formulaire de demande de stage ont pour origine l'étudiant.

Les informations contenues dans le formulaire de contact ont pour origine toute personne.

Les logs de connexion ont pour origine le système.

Enfin, les statistiques Piwik (Matomo) ont pour origine l'outil Piwik (Matomo).

La Commission considère ainsi que les informations collectées au sein dudit traitement sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément à 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 réalisée par le biais des mentions légales du site internet.

Ces mentions n'ayant pas été jointes à la demande, la Commission rappelle que l'information des personnes concernées doit impérativement être conforme aux dispositions de 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 des personnes concernées par le traitement s'exerce par voie postale ou par courrier électronique auprès du Délégué à la protection des données personnelles.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit intervenir dans le mois suivant la réception de la demande.

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.

Sous cette condition, la Commission considère que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 la Loi n° 1.165 du 23 décembre 1993.

V. Sur les personnes ayant accès au traitement

Les personnes pouvant avoir accès aux informations sont :

- les responsables du site internet (chacun pour la rubrique qui le concerne) : inscription, modification, mise à jour du contenu du site internet ;
- le responsable des actualités : gestion du contenu ;
- le prestataire : tout accès à des fins de maintenance du site ;
- les administrateurs DSIO : mise à jour, modification, suppression du système.

Au vu des missions et attributions de chacune des personnes ayant accès au traitement, la Commission considère que les accès au traitement sont justifiés, et donc conformes aux dispositions de la Loi n° 1.165 du 23 décembre 1993.

En ce qui concerne le prestataire, elle rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit sous-traitant est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

VI. Sur les rapprochements et interconnexions

Le responsable de traitement indique que le présent traitement fait l'objet de trois rapprochements avec les traitements ayant respectivement pour finalité « *Gestion des Ressources Humaines et paie* », « *Gestion de la messagerie professionnelle du CHPG* » et « *Gestion des services de téléphonie du CHPG* ».

La Commission constate que ces traitements ont été légalement mis en œuvre.

Elle note par ailleurs que le site internet du CHPG est interconnecté avec un autre site internet administré par le Gouvernement Princier, n'ayant fait l'objet d'aucune formalité auprès de la Commission.

Aussi, elle interdit ladite interconnexion tant que le site dont s'agit n'a pas reçu un avis favorable de la Commission.

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'observations.

La Commission rappelle toutefois 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.

Elle recommande par ailleurs que la sécurité du « *Captcha* » utilisé dans l'ensemble des formulaires du site soit renforcée.

Enfin, la Commission rappelle que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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 les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité, les adresses et coordonnées ainsi que les informations relatives à la formation, aux diplômes et à la vie professionnelle sont conservées la durée de la relation du contrat de travail.

Les informations relatives au paiement en ligne et les informations contenues dans les formulaires (candidature, demande de stage et contact) ne sont pas conservées sur le site.

Les logs de connexion sont conservés 1 an.

Enfin, les statistiques sont conservées 13 mois en ce qui concerne l'identification des requêtes, 6 mois en ce qui concerne la référence des requêtes et 30 minutes en ce qui concerne les sessions.

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 :

- l'information des personnes concernées doit impérativement être effectuée conformément à l'article 14 de la Loi n° 1.165 ;
- la réponse au droit d'accès doit intervenir dans le mois suivant la réception de la demande ;
- 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.

Interdit l'interconnexion avec le site internet administré par le Gouvernement Princier tant que ce dernier n'a pas reçu un avis favorable de la Commission.

Recommande que la sécurité du « *Captcha* » utilisé dans l'ensemble des formulaires du site soit renforcée.

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 Centre Hospitalier Princesse Grace, du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion du site internet du CHPG* ».**

Le Président

Guy MAGNAN