

Délibération n° 2018-160 du 17 octobre 2018

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 de la facturation des repas au self* »

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° 918 du 27 décembre 1971 sur les établissements publics ;

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 l'Arrêté Ministériel n° 86-620 du 10 novembre 1986 portant établissement du règlement intérieur du Centre Hospitalier Princesse Grace, modifié ;

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 11 juillet 2018, portant sur la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la facturation des repas au self* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 7 septembre 2018, 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 17 octobre 2018 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 de la facturation des repas au self* ».

Il indique que les personnes concernées sont le personnel du C.H.P.G., le prestataire, les stagiaires et les élèves infirmiers.

Les fonctionnalités sont les suivantes :

- l'accès à la liste des repas qui permet de visualiser et de supprimer les repas et les plats ;
- la gestion des comptes qui permet de voir et de créditer un compte self ;
- le journal des encaissements ainsi que les statistiques qui permettent d'imprimer les encaissements, les statistiques effectuées à une date ou entre deux dates et les statistiques effectuées sur une période ou une journée ;
- le ticket automatique message client qui permet d'activer l'impression systématique d'un ticket après chaque encaissement et d'afficher un message personnalisé sur la fenêtre « *client* » ;
- la désignation des plats qui permet de modifier l'intitulé d'un ou plusieurs plats ;
- le type de paiement qui est soit immédiat pour les personnes extérieures (espèces, chèque, carte bancaire) ou différé pour les agents du C.H.P.G. (numéro de badge).

Après étude du dossier, la Commission considère que le traitement a également les fonctionnalités suivantes :

- le planning d'affectation du personnel à la caisse ;
- la conservation des repas liés aux numéros de badge en cas de problème d'hygiène.

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**

Ce traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement sans que soient méconnus les droits et libertés fondamentaux des personnes concernées.

En effet, le traitement mis en place par le C.H.P.G. va permettre d'assurer la gestion de la facturation des repas du personnel de l'établissement mais aussi du prestataire, des stagiaires et des élèves infirmiers.

En outre, les droits des personnes concernées sont respectés, comme cela est examiné au point IV de la présente délibération.

Par conséquent, 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**

Les informations nominatives objets du présent traitement sont :

- identité : matricule de l'agent, numéro de badge ;
- caractéristiques financières : montant du repas (paiement par badge), total montant à rendre (paiement espèce), impression ticket repas (paiement espèce), solde positif ou négatif ;
- consommation de biens et services : plats du repas ;
- journal des encaissements : date et heure du plateau servi ;
- statistiques : total des repas servis, total des plats servis, nombre de plats par famille, détails par plats.

Concernant ces dernières données, la Commission constate qu'elles sont anonymisées.

Les informations relatives à l'identité ont pour origine le traitement ayant pour finalité « *Gestion des ressources Humaines et Paie* ».

Les informations relatives aux caractéristiques financières et à la consommation de biens et services ainsi que le journal des encaissements et les statistiques ont pour origine l'application du self.

La Commission considère ainsi que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions des articles 10-1 et 12 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 au moyen d'un document spécifique.

Ce document n'ayant pas été joint 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 auprès de la Direction du CHPG.

La Commission constate ainsi 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**

Le traitement est interne au CHPG.

Les personnes pouvant avoir accès aux informations sont :

- le personnel du self : tout accès;
- les agents de la Direction des Systèmes d'Information et Organisation (DSIO) habilités : à des fins de maintenance des systèmes.

A cet égard, la Commission constate que l'identification et l'authentification se font sur un poste client qui contient l'application self et que cette dernière semble rester synchronisée avec la précédente identification et authentification.

Si tel était le cas, elle demande que chaque caissier se déconnecte lors de tout changement de poste et que le suivant se connecte avec son propre identifiant et mot de passe pour accéder à l'application self.

Sous cette condition, la Commission considère que les accès susvisés sont justifiés.

**VI. Sur les rapprochements et interconnexions**

Le responsable de traitement indique que le présent traitement est interconnecté avec le traitement ayant pour finalité « *Gestion des Ressources Humaines et Paie* ».

La Commission constate que ce traitement a été 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'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 rappelle par ailleurs 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 la durée de conservation**

Les informations nominatives relatives à l'identité sont conservées 5 ans à compter du départ du salarié.

Les informations nominatives relatives aux caractéristiques financières sont conservées 5 ans après la destruction du montant du repas.

Les informations relatives au journal des encaissements sont conservées 3 mois après la distribution du repas.

Enfin, les statistiques sont conservées de manière illimitée.

Par ailleurs, la Commission demande que les logs de connexion des personnes affectées à la caisse soient conservés 1 an.

Considérant ces derniers, la Commission rappelle que les identifiants ne doivent être conservés que tant que la personne est en poste.

Par ailleurs, s'agissant du mot de passe, elle recommande au responsable de traitement de ne le conserver que 3 mois ou bien d'adopter 9 caractères (majuscule, minuscule, alphanumérique) s'il désire le conserver 6 mois.

Sous ces conditions, la Commission considère que les durées sont conformes aux exigences légales.

### **Après en avoir délibéré, la Commission :**

**Considère que** le traitement a également pour fonctionnalités le planning d'affectation du personnel à la caisse et la conservation des repas liés aux numéros de badge en cas de problème d'hygiène.

### **Rappelle que :**

- l'information des personnes concernées doit impérativement être effectuée conformément à l'article 14 de la Loi n° 1.165 ;
- 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 ;
- les identifiants ne doivent être conservés que tant que la personne est en poste.

**Demande que :**

- tout utilisateur de l'application « *Self* » s'authentifie à chaque connexion à l'application et se déconnecte en fin d'utilisation permettant ainsi à l'utilisateur suivant de s'identifier et s'authentifier afin de se connecter au système ;
- les logs de connexion des personnes affectées à la caisse soient conservés 1 an.

**Recommande** au responsable de traitement de ne conserver le mot de passe que 3 mois ou bien d'adopter 9 caractères (majuscule, minuscule, alphanumérique) s'il désire le conserver 6 mois.

**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 de la facturation des repas au self* ».**

Le Président

Guy MAGNAN