Délibération n° 2022-100 du 20 juillet 2022

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 des badges des bâtiments publics* »

exploité par le Service de Maintenance des Bâtiments Publics (SMBP)

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° 4.683 du 20 janvier 2014 portant création d'un Service de Maintenance des Bâtiments Publics ;

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 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 demande d'avis déposée par le Ministre d'Etat le 19 mai 2022 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des badges des bâtiments publics » ;*

Vu la prorogation du délai d'examen de ladite demande d'avis notifiée au responsable de traitement 18 juillet 2022, 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 juillet 2022 portant examen du traitement automatisé susvisé.

## La Commission de Contrôle des Informations Nominatives,

## Préambule

Le Service de Maintenance des Bâtiments Publics (SMBP) est chargé de réaliser et suivre l'état et la maintenance des bâtiments publics. Il a ainsi, parmi ses missions, « *la participation à la maîtrise des accès aux bâtiments, notamment à la gestion des clés permettant leur ouverture et fermeture par les responsables de site, l'accès aux personnels techniques (comme les sociétés d'entretien et de ménage), mais aussi la limitation d'accès à certains équipements comme les ascenseurs dans les écoles* ».

Afin de mener à bien ces missions, le SMBP souhaite mettre en place un système de gestion de badges qui lui permet, dès lors qu'un responsable d'un bâtiment, d'un local ou d'un établissement scolaire lui en fait la demande, d'installer les équipements (UTL et lecteur de badges) et de former les référents (personnes désignées pour gérer les badges) à l'utilisation, sur leur périmètre uniquement, dudit système.

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 des badges des bâtiments publics* ».

Les personnes concernées sont les « *fonctionnaires et agents de l'Etat habilités* », les « *prestataires habilités à accéder aux bâtiments publics* » et « *les personnels de la DSI habilités* ».

Enfin, les fonctionnalités sont les suivantes :

- la gestion des accès à la solution ;
- la gestion des badges par le référent du bâtiment ou le SMBP, selon le cas (création, modification et suppression des badges, désactivation et suppression des badges perdus) ;
- le suivi de l'utilisation des badges ;
- le début de preuve, en cas d'incident/d'infractions, le cas échéant.

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 présent traitement est tout d'abord justifié par le respect d'une obligation légale puisqu' il « *s'inscrit dans le cadre des missions du SMBP telles que définies, par l'Ordonnance Souveraine n° 4.683 du 20 janvier 2014 portant création d'un Service des Bâtiments Publics* ».

Il précise que « *Dans ce sens, il entre dans une des missions particulières du SMBP « de préparer sur les plans administratifs et techniques les interventions liées à l'exécution des travaux de grosses réparations, d'amélioration et d'entretien des immeubles, y compris les équipements techniques, à usage administratif, culturel, pénitentiaire ou accessoirement d'habitation relevant du domaine public et du domaine privé de l'Etat », et de surveiller les travaux précités, de les contrôler et de préparer leur règlement. Il a, en pratique, une mission générale de maintenance et de surveillance de l'Etat des bâtiments publics* ».

Le responsable de traitement indique par ailleurs que le traitement est également justifié par la réalisation d'un intérêt légitime, sans que ne soient méconnus les droits et libertés fondamentaux des personnes concernées.

La Commission prend ainsi acte que « *Le présent traitement permet de veiller à ce que seules les personnes autorisées puissent ouvrir/fermer les bâtiments publics, puissent accéder aux bâtiments après leur fermeture ou activer certains équipements dans un objectif de sécurité des biens et des personnes* ».

Elle note enfin que « *Le traitement ne comporte pas d'informations nominatives sur les personnes occupant les locaux* » et qu'il « *n'a pas pour objet de surveiller les personnes concernées* ».

Au vu de ce qui précède, la Commission considère que ce 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 nominatives traitées

Les informations nominatives traitées sont :

- identité : nom et prénom du référent ou de l'administrateur, nom, prénom ou entreprise pour la personne disposant d'un badge ;
- adresses et coordonnées : email du référent (uniquement pour notification d'alarme) ;
- vie professionnelle : fonction du référent ou de l'administrateur ;
- données d'identification électronique : login et mot de passe du référent ou de l'administrateur ;
- informations temporelles : logs de connexion ;
- éléments de création du badge : date de création/validation, ID, numéro de badge ou code du badge, statut (clé validé/invalide/obsolète), état du badge (actif/désactivé), usage, groupe (porte, horaire d'accès), nombre d'usage le cas échéant ;
- mouvements du badge : date, heure, activité (ouverture/fermeture de porte, appel de cabine d'ascenseur).

Les informations relatives à l'identité et à la vie professionnelle ont pour origine le responsable du site concerné, la personne concernée ou la Direction des Systèmes d'Information (DSI).

L'adresse email a pour origine le responsable du site concerné.

Les données d'identification électronique ont pour origine le SMBP pour le login et les personnes concernées pour le mot de passe.

Enfin, les logs de connexion, les éléments de création du badge et les mouvements du badge ont pour origine le système.

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 « *Notice d'information lors de la création du compte* ».

A l'analyse de ce document, la Commission considère que celui-ci est conforme 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 voie postale ou par courrier électronique auprès du Service de Maintenance des Bâtiments Publics.

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

Par ailleurs, 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° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, la Commission constate 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***

Le responsable de traitement indique que les Autorités administratives et ou judiciaires dans le cadre de leurs missions légalement conférées peut être destinataire des informations.

La Commission estime ainsi que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

Elle considère donc que ces transmissions sont conformes aux exigences légales

- ***Sur les personnes ayant accès au traitement***

Les personnes habilitées à avoir accès au traitement sont les suivantes :

- les administrateurs de la solution au sein du SMBP: tout accès ;
- le responsable/référent du site concerné : tout accès sur le périmètre du site ;
- le personnel de la DSI ou tout intervenant sous son autorité : à des fins de maintien en condition opérationnelle (MCO), de maintien en condition de sécurité (MCS), de la maintenance et du maintien de l'infrastructure ;
- le prestataire : maintenance et mise à jour des bases de données et de l'applicatif.

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

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 prestataire 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 interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet de trois rapprochements avec les traitements ayant respectivement pour finalité :

- « *Gestion de la messagerie professionnelle* » ;
- « *Gestion des habilitations et des accès au Système d'information par l'Active Directory* » ;
- « *Assistance aux utilisateurs par le Centre de Service de la DSI* ».

Le responsable de traitement indique en outre que ledit traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité « *Gestion et analyse des évènements du système d'information* ».

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

## VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations appellent plusieurs observations.

La Commission demande ainsi que les demandes de badges soient tracées.

Elle demande également qu'en cas d'utilisation d'identifiants génériques ou partagés, cette utilisation soit validée par la hiérarchie et qu'une traçabilité soit mise en place afin d'identifier tout acteur.

La Commission rappelle par ailleurs 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 que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception, conformément à la délibération n° 2010-13 du 3 mai 2010.

La Commission rappelle enfin 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 les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité, à l'email et à la vie professionnelle ainsi que les données d'identification électronique sont conservées tant que la personne est habilitée à avoir accès au traitement.

Les logs de connexion sont conservés 12 mois.

Les éléments de création du badge sont conservés 12 mois après la dernière utilisation du badge.

Enfin, les informations relatives aux mouvements du badge sont conservées 12 mois glissant.

La Commission considère ainsi 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 :**

- la réponse au droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;
- la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire
- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort ;
- la copie et l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

**Demande :**

- que les demandes de badges soient tracées ;
- qu'en cas d'utilisation d'identifiants génériques ou partagés, cette utilisation soit validée par la hiérarchie et qu'une traçabilité soit mise en place afin d'identifier tout acteur.

**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 des badges des bâtiments publics* ».**

Le Président

Guy MAGNAN