Délibération n° 2022-095 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 accès à distance au Système d'Information de la Mairie de Monaco* »

présenté par la Commune de Monaco

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, et notamment son article 10 ;

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 du 28 janvier 1981 et son protocole additionnel ;

Vu la Loi n° 1.096 du 7 août 1986 portant statut des fonctionnaires de la Commune, modifiée ;

Vu la Loi n° 1.165 du 23 décembre 1993, modifiée, 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, susvisée ;

Vu l'Ordonnance Souveraine n° 4.934 du 22 août 2014 relative aux obligations déontologiques des fonctionnaires de la Commune ;

Vu l'Arrêté Municipal n° 2019-559 du 14 février 2019 portant application de l'Ordonnance Souveraine n° 4.934 du 22 août 2014 relative aux obligations déontologiques des fonctionnaires de la Commune ;

Vu l'Arrêté Municipal n° 2019-561 du 14 février 2019 portant application de l'Ordonnance Souveraine n° 4.934 du 22 août 2014 relative aux obligations déontologiques des fonctionnaires de la Commune ;

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 la Commune de Monaco le 3 mai 2022 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des accès à distance au Système d'Information de la Mairie de Monaco* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 1er juillet 2022, 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 20 juillet 2022 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Commune de Monaco exploite un système d'information permettant à ses Services de fonctionner conformément aux missions qui leur sont dévolues.

Afin de maîtriser l'ensemble des accès aux ressources de l'Administration Communale, elle souhaite mettre en place un traitement ayant pour objectif d'assurer la sécurité des accès à distance audit Système d'Information par le biais d'une solution adaptée en évitant le recours à des logiciels de prise en main à distance non sécurisés et non maîtrisés.

Ledit traitement, 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, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Gestion des accès à distance au Système d'Information de la Mairie de Monaco* ».

Les personnes concernées sont les fonctionnaires de la Commune, les agents de la Commune, les suppléants et les prestataires avec accès à distance.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

- permettre un accès à distance à certains environnements précis et restreints du Système d'Information de la Mairie de Monaco de manière sécurisée ;
- disposer d'informations sur les prestataires permettant d'examiner les demandes, d'implémenter la procédure et son fonctionnement ;
- assurer l'implémentation de la solution, son activation, sa désactivation et sa suppression ;
- lier les accès spécifiques du bastion à la gestion des habilitations ;
- analyser les besoins de maintenance de la solution et communiquer avec les personnes intéressées en cas d'intervention sur le Bastion (exemple : maintenance) ;
- permettre la traçabilité des sessions et l'imputabilité des actions ;
- vérifier, *a posteriori*, si nécessaire, les actions réalisées par les utilisateurs de la solution et disposer, le cas échéant, de preuves ou de début de preuves si de besoin ;
- conserver des éléments retraçant la réalisation des opérations réalisées par les agents à des fins, le cas échéant, de vérification et de compréhension d'une situation donnée ;
- assurer les opérations de suivi et de maintenance des équipements et ressources du Bastion ;
- établir des statistiques, rapports d'évaluation et d'analyse.

La Commission prend acte des précisions du responsable de traitement selon lesquelles les statistiques et les rapports sont non nominatifs.

Au vu de ce qui précède, 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.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement est justifié à la fois par le respect d'une obligation légale à laquelle il est soumis et par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnait ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

Il précise à cet effet que *« La mise en place de cet outil résulte des attributions du Service Informatique de la Commune et particulièrement du Responsable de Sécurité des Systèmes d'Information ».*

Le responsable de traitement mentionne en outre que « *L'Arrêté Municipal n° 2019-561 du 14 février 2019 portant application de l'Ordonnance Souveraine n° 4.934 du 22 août 2014 relative aux obligations déontologiques des fonctionnaires de la Commune ajoute des obligations aux fonctionnaires, outre celles déjà consacrées dans la Loi n° 1.096 du 7 août 1986 portant statut des fonctionnaires de la Commune, modifiée. Ainsi, les fonctionnaires de la Commune chargés de la sécurité des informations traitées au sein de leur service ou responsables des systèmes d'information ou encore chargés de la sécurité et de l'exploitation des systèmes d'information, sont tenus de respecter les obligations professionnelles énoncées dans la Politique de Sécurité des Systèmes d'Information de la Commune annexée à l'arrêté susvisé ».*

La Commission note également que *« Concernant les agents de la Commune qui ne sont pas visés par la Loi n° 1.096 du 7 août 1986, la même obligation est consacrée dans leur contrat de travail* ».

Le responsable de traitement indique que « De plus, l'Arrêté Municipal n° 2019-559 du 14 février 2019 portant application de l'Ordonnance Souveraine n° 4.934 du 22 août 2014 relative aux obligations déontologiques des fonctionnaires de la Commune ajoute lui aussi des obligations aux fonctionnaires, outre celles déjà consacrées dans l'Ordonnance n° 1.096 du 7 août 1986, portant statut des fonctionnaires de la Commune, modifiée. Ainsi, les fonctionnaires de la Commune intervenant dans le cadre du bon fonctionnement et de la sécurité des systèmes d'information de la Commune, dénommés « Administrateurs réseaux et systèmes d'information », sont tenus de respecter les obligations professionnelles énoncées dans la Charte Administrateur Réseaux et Systèmes d'Informations annexée à l'arrête susvisé ».

Enfin, la Commission prend acte que « *Concernant les agents de la Commune qui ne sont pas visés par la Loi n° 1.096 du 7 août 1986, la même obligation leur est soumise. Ils devront signer un accusé de réception les engageant à respecter la Charte Administrateur Réseaux et Systèmes d'Information* ».

Au vu de ce qui précède, la Commission 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 traitées sont les suivantes :

- identité : nom, prénom ;

- adresses et coordonnées du personnel communal : téléphone, email ;
- formation, diplômes, vie professionnelle : fonction, service, société ;
- données d'identification électronique : login et mot de passe ;
- informations temporelles : logs de connexion sur le Bastion ;
- informations relatives à la demande : projet, raison de l'accès, date de début, date de fin, date de validation ;
- données de connexion : serveur, lieu et adresse IPs publique depuis laquelle le prestataire devra ouvrir la connexion (IPs entreprise).

Les informations relatives à l'identité, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle ont pour origine soit l'Active Directory soit le formulaire rempli par le prestataire.

Les données d'identification électronique ont pour origine l'Active Directory.

Les informations temporelles ont pour origine le système.

Enfin, les informations relatives à la demande et les données de connexion ont pour origine le formulaire rempli par le prestataire.

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*

Le responsable de traitement indique que l'information préalable s'effectue par le bais d'une rubrique dédiée à la protection des données qui s'affiche avant même que l'utilisateur puisse procéder à ses actions.

A l'analyse du document joint au dossier, la Commission considère que les modalités d'information préalable des personnes sont conformes aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

➢ *Sur l'exercice du droit d'accès*

Le responsable de traitement indique que le droit d'accès s'exerce par voie postale ou par courrier électronique auprès du Data Protection Office (DPO).

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.

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 habilitées à avoir accès au traitement sont :

- le Responsable de Sécurité des Systèmes d'Information (RSSI) : tous droits (en mode audit et en approbation) dans le cadre de ses opérations de validation et de contrôle ;
- les Administrateurs internes de la solution : tous droits ;
- les Auditeurs Mairie : droits d'audit de la session en cours et terminées ;
- le prestataire informatique : tous droits à des fins d'administration des systèmes limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestations de services.

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

En ce qui concerne le prestataire, la Commission rappelle toutefois 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 rapprochements et les interconnexions

Le responsable de traitement indique que le présent traitement fait l'objet de deux rapprochements avec les traitements ayant respectivement pour finalité « *Gestion des techniques automatisées d'information et de communication* », et « *Gestion de la messagerie professionnelle* », légalement mis en œuvre.

La Commission en prend acte et considère que ces rapprochements sont conformes aux exigences légales.

Le responsable indique également que le traitement est interconnecté avec le traitement ayant pour finalité « *Gestion des habilitations et des accès au Système d'Information* », soumis concomitamment.

A cet égard, la Commission rappelle que ce rapprochement ne peut être effectué qu'entre 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'observations particulières.

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.

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 données sont conservées dans le traitement 12 mois glissants.

Il précise par ailleurs que les données relatives à l'ouverture des droits d'accès des utilisateurs sont conservées jusqu'au départ de la personne ou pour la durée du contrat de prestations la liant à la Mairie de Monaco.

A cet égard, la Commission considère que ces droits sont maintenus uniquement tant que ces utilisateurs restent habilités.

Au vu de ce qui précède, 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 ;

- que les droits d'accès des utilisateurs sont maintenus uniquement tant que ces utilisateurs restent habilités.

Rappelle que :

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

- tout rapprochement ne peut être effectué qu'entre des traitements légalement mis en œuvre ;

- 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.

A la condition 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 la Commune de Monaco du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des accès à distance au Système d'Information de la Mairie de Monaco* ».**

Le Président

Guy MAGNAN