

Délibération n° 2022-103 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

« *Sécurisation des accès à distance au système d'information de la Mairie pour les flottes nomades BYOD et professionnelles* »,

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 ;

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 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 et 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 ayant pour finalité « *Sécurisation des accès à distance au système d'information de la Mairie pour les flottes nomades BYOD et professionnelles* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 1<sup>er</sup> 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 permet à ses fonctionnaires et agents ainsi qu'aux élus du Conseil Communal, qui le demandent, de déployer sur leurs terminaux personnels ou professionnels (smartphones et mobiles) une application « *afin de permettre l'accès à distance sécurisé à des contenus identifiés localisés sur le Système d'Information de la Mairie de Monaco. Ces contenus pourront être du mail, des applications Web et toute application paramétrée pour être accessible [par la solution] au fur et à mesure des besoins exprimés* ».

Ainsi, « *il s'agit de créer sur les terminaux des personnes concernées et, qui en ont besoin, un conteneur permettant de sécuriser l'accès aux applications autorisées par la Commune. Seules les applications ciblées comme pouvant être mises à disposition des agents peuvent être installées dans le conteneur* ».

Ainsi, le traitement y relatif est 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 présent traitement a pour finalité « *Sécurisation des accès à distance au système d'information de la Mairie pour les flottes nomades BYOD et professionnelles* ».

Il concerne les fonctionnaires et agents de la Commune ainsi que les élus du Conseil Communal qui souhaitent disposer de l'application.

Les fonctionnalités du traitement sont :

- création d'un compte sur la solution pour mettre en place les connectivités ;
- enrôlement des terminaux dans l'interface d'administration de la solution ;
- authentification des utilisateurs pour un accès à distance sécurisé ;
- gestion des licences de la solution dans une interface Home Machine (IHM) de management ;
- établissement de statistiques et tableaux de bord.

Il ressort des précisions apportées par le responsable de traitement que lesdites statistiques sont anonymes. Il appert par ailleurs que l'enrôlement des terminaux dans l'interface d'administration de la solution génère la création d'un ticket d'enrôlement unique.

La Commission constate 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 justifié par le respect d'une obligation légale à laquelle il est soumis ainsi que par la réalisation d'un intérêt légitime, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

Il précise notamment que la mise en place de l'outil résulte des attributions du Service Informatique de la Commune et, plus particulièrement, du Responsable de Sécurité des Systèmes d'Information. Le Service Informatique de la Commune doit en effet assurer la disponibilité des ressources informatiques en environnement sécurisé.

En outre, il est indiqué que le présent traitement est conforme à la Politique de Sécurité des Systèmes d'Information de la Commune (PSSI-C) annexée à l'Arrêté Municipal n° 2019-561 du 14 février 2019, étant précisé que cela participe nécessairement à sa sécurité, en ce que ladite PSSI-C impose des obligations procédurales dans la gestion et la révocation des droits d'accès aux systèmes d'information, la gestion des privilèges, etc.

Par ailleurs, le responsable de traitement se fonde sur la Charte Administrateur Réseaux et Système d'Information qui impose, aux utilisateurs et aux administrateurs des systèmes d'information de la Commune, des obligations propres à leurs fonctions. Il souligne de plus 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 réception les engageant à respecter la Charte Administrateur Réseaux et Système d'Information* ».

En toute fin, il est indiqué qu'un formulaire de consentement de déploiement de l'application est signé par l'utilisateur avant l'enrôlement des terminaux personnels dans l'interface de l'outil. La personne concernée atteste ainsi être informée que le personnel dûment habilité du Service Informatique ne pourra accéder qu'aux données professionnelles contenues dans la bulle applicative déployée sur son téléphone. Il est précisé, qu'en aucun cas, le Service Informatique ne pourra accéder aux informations de nature personnelle contenues dans le téléphone mobile.

En ce qui concerne les titulaires de terminaux professionnels il ressort des précisions apportées par le responsable de traitement qu'une note d'information leur est remise, laquelle leur indique que « *[S]’agissant de ressources strictement réservées à un usage professionnel, le personnel dûment habilité du Service Informatique sera en mesure d’accéder à l’ensemble des données contenues dans le téléphone professionnel mis à disposition de l’utilisateur, dans le cadre de ses missions de gestion de la sécurité de ses systèmes d’information* ».

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 traitées**

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité : nom, prénom ;
- coordonnées : email professionnel, pays, numéro de téléphone mobile ;
- informations temporelles : adresse mac, logs de connexion, date de la dernière connexion, durée totale de connexion ;
- identification du téléphone : type de téléphone (Android, IOS), marque du téléphone, numéro IMEI, opérateur ;
- éléments administratifs de suivi : date d'enregistrement, numéro de licence, date d'initialisation, date de fin, statut (active).

La Commission prend acte que « *les données de roaming des utilisateurs de la solution ne sont pas accessibles aux administrateurs de la solution* ».

S'agissant du pays, il ressort des compléments d'information apportés par le responsable de traitement que seul l'indicatif pays associé au numéro de mobile est collecté.

La Commission relève par ailleurs que l'identifiant technique de l'utilisateur, le nom, le prénom, le nom d'affichage, l'email et le mot de passe des administrateurs de la solution sont également collectés.

En outre, elle prend acte que l'enrôlement des terminaux n'intervient que sur rendez-vous pris auprès du Service Informatique générant, de ce fait, un ticket d'enrôlement par la solution ainsi qu'un code pin éphémère. Ce dernier est communiqué, par l'administrateur, à la personne concernée lors de l'enrôlement du terminal.

Les informations relatives à l'identité de l'utilisateur, à son email et celles relatives aux administrateurs de la solution ont pour origine le traitement relatif à la gestion des habilitations.

Il est précisé que l'email professionnel, l'indicatif pays du numéro de téléphone mobile et les informations concernant l'identification du téléphone sont fournis par la personne concernée.

Enfin, les informations temporelles et les éléments administratifs de suivi sont issus du système.

La Commission considère 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 mention sur le document de collecte (formulaire de consentement au déploiement de la solution) ainsi que par une rubrique propre à la protection des données accessible en ligne.

S'agissant du formulaire remis aux personnes concernées, la Commission constate que celui-ci contient une mention conforme aux dispositions de l'article 14 de la Loi n° 1.165.

Elle rappelle à cet égard que la rubrique propre à la protection des données, accessible en ligne, devra également respecter les dispositions de l'article 14, susvisé.

Il ressort enfin des précisions apportées par le responsable de traitement qu'une note d'information est remise aux personnes munies d'un terminal professionnel sur lequel est déployée la solution. La Commission constate que cette dernière comporte une mention d'information conforme aux dispositions de l'article 14 de la Loi n° 1.165.

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

Le droit d'accès est exercé par voie postale ou par courrier électronique auprès du Data Protection Officer.

La Commission prend acte de l'existence d'une procédure dédiée.

## **V. Sur les destinataires et les personnes ayant accès au traitement**

Les accès sont définis comme suit :

- les Administrateurs de la solution du Service Informatique : tout accès notamment pour l'enrôlement des terminaux et la création des comptes ;
- les Administrateurs de l'infrastructure : accès aux logs de connexion à partir de la console de management de la solution ;
- le prestataire : accès à des fins d'administration des systèmes limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestations de services.

En ce qui concerne le prestataire, la Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 les droits d'accès de ce dernier doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestations de services. 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.

La Commission considère que ces accès sont justifiés.

## **VI. Sur les rapprochements et les interconnexions**

Le responsable de traitement indique que le présent traitement fait l'objet de deux interconnexions 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 interconnexions sont conformes aux exigences légales.

Le responsable de traitement indique également que le traitement est rapproché et interconnecté avec le traitement « *Gestion des habilitations et des accès au système d'information* » et est interconnecté avec le traitement ayant pour finalité « *Gestion des accès à distance au système d'information de la Mairie de Monaco* », tous deux soumis concomitamment.

A cet égard, la Commission rappelle que ce rapprochement et ces interconnexions ne peuvent être effectués 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'observation.

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 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 la durée de conservation**

Le responsable de traitement indique que les informations sont conservées jusqu'à la suppression de l'application, à la suite du départ de l'intéressé ou, à sa demande en ce qui concerne les données d'identité, de coordonnées, d'identification du téléphone et les éléments administratifs de suivi de l'utilisateur.

Il précise par ailleurs que les informations temporelles et les données de connexion sont supprimées tous les 12 mois, glissants.

La Commission relève, en outre, qu'en cas de départ de l'utilisateur, l'accès au service est supprimé sans préavis.

Enfin, s'agissant de la durée de conservation des tickets d'inscription, la Commission considère que ces derniers peuvent être conservés :

- au maximum 6 mois suivant le refus de l'inscription ;
- tant que les utilisateurs bénéficient de cet accès à distance sécurisé.

S'agissant des données relatives à l'identifiant technique de l'utilisateur, aux nom, prénom, nom d'affichage, email et mot de passe des administrateurs de la solution, elle rappelle que ces dernières sont conservées tant que la personne est habilitée à avoir accès au traitement.

Sous cette réserve, la Commission considère que ces durées de conservation sont conformes aux exigences légales.

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

##### **Rappelle que :**

- tout rapprochement ou interconnexion ne peut être effectué qu'entre des traitements légalement mis en œuvre ;
- les données relatives aux administrateurs de la solution sont conservées tant que la personne est habilitée à avoir accès au traitement ;
- 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 ;

##### **Considère que les tickets d'inscription peuvent être conservés :**

- au maximum 6 mois suivant le refus de l'inscription ;
- tant que les utilisateurs bénéficient de cet accès à distance sécurisé.

**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 la Commune de Monaco, du traitement automatisé d'informations nominatives ayant pour finalité « *Sécurisation des accès à distance au système d'information de la Mairie pour les flottes nomades BYOD et professionnelles* ».**

Le Président

Guy MAGNAN