Délibération n° 2019-138 du 18 septembre 2019

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 messagerie électronique professionnelle Office 365* »,

exploité par la Direction des Réseaux et des Systèmes d'Information

présenté par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne 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 d'informations nominatives ayant pour finalité « Gestion de la messagerie électronique utilisée à des fins de surveillance ou de contrôle » ;

Vu la délibération n° 2015-111 du 18 novembre 2015 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les traitements automatisés ou non automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique utilisée à des fins de surveillance ou de contrôle* » ;

Vu la demande d'avis déposée par le Ministre d'Etat, le 7 juin 2019, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion de la messagerie électronique professionnelle Office 365* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 5 aout 2019, 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 18 septembre 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

L'Administration souhaite mettre à disposition des fonctionnaires, agents de l'Etat et prestataires qui ne disposent pas d'un terminal au sein de l'Administration, une messagerie professionnelle accessible depuis tout terminal via Internet. Il est précisé que ces derniers « *pourront ainsi disposer d'une adresse mail en rapport avec le Gouvernement Monégasque et attribuée par ce dernier* ».

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 « *Gestion des accès à distance au Système d'information du Gouvernement* ».

Il concerne les fonctionnaires et agents de l'Etat, ainsi que les prestataires, qui ne disposent pas de terminaux (exemple PC) fournis par l'Administration.

Les fonctionnalités du traitement sont :

- Gérer les comtes de messagerie O365 de leur création à leur administration ;
- Echange de messages électroniques en interne ou avec l'extérieur ;
- Historisation des messages électroniques entrants et sortants ;
- Gestion des contacts de la messagerie électronique ;
- Gestion des dossiers de la messagerie et des messages archivés ;
- Etablissement et lecture de fichiers journaux ;
- Gestion des habilitations d'accès à la messagerie ;
- Gestion de l'agenda ;
- Etablissement de preuves en cas de litige avec un agent ;
- Assurer la qualité et le fonctionnement opérationnel de la messagerie ;
- Veiller au maintien en condition de sécurité de l'application ;
- Etablir des statistiques à des fins de reporting.

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 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 est indiqué que traitement concourt à *« l'intégration de l'ensemble des agents et fonctionnaires de l'Etat »*, *« en mettant à la disposition de l'ensemble de ses agents des moyens de communication actuels »,* par le biais d'un *« outil qui offre des fonctionnalités répondant aux préoccupations de l'Administration tout en assurant la sécurité des échanges, des systèmes d'information et réseaux (…) ».*

Il est en outre précisé que ce traitement est conforme à la politique de sécurité des systèmes d'information de l'Etat (PSSIE), annexée à l'Arrêté Ministériel n° 2017-56 du 1er février 2017, et s'intègre dans l'application de la Charte des systèmes d'information de l'Etat annexée à l'Arrêté Ministériel n° 2015-703 du 26 novembre 2015, et de la Charte « *Administrateur réseaux et système d'information de l'Etat* », qui imposent aux utilisateurs et admirateurs des systèmes d'Information de l'Etat des obligations propres à leurs fonctions.

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 :

En ce qui concerne le destinataire/expéditeur/contact des messages :

- identité : nom, prénom ;
- coordonnées : email.

En ce qui concerne l'administrateur :

- identité : nom, prénom ;
- nom d'utilisateur : adresse email ;
- vie professionnelle : fonction, Département, Direction, Service, statut, rôle (user), licence ;
- coordonnées professionnelles : téléphone, email ;
- données d'identification électronique : login, mot de passe (chiffré) ;
- informations temporelles et logs de connexion: connexion au système, horodatage, logs de connexion ;
- données de connexion : logs de connexion (OS, navigateur et version de l'appareil utilisé pour l'évènement de connexion, adresse IP, valeur d'accès interne/externe, objectID, nom de la commande.

En ce qui concerne l'utilisateur de la messagerie :

- identité : nom, prénom ;
- vie professionnelle : statut – rôle (admin)/licence ;
- coordonnées professionnelles : email ;
- données d'identification électronique : login, mot de passe (chiffré) ;
- informations temporelles et log de connexion : connexion au système (Date et heure à l'heure UTC au moment où l'utilisateur a effectué l'activité), logs de connexion (OS, navigateur et version de l'appareil utilisé pour l'évènement de connexion, adresse IP, valeur d'accès interne/externe, objectID, nom de la commande ;
- message : messages et contenu ;
- informations en lien avec les messages : type de contenu, objet, dossier de classement, date et heure d'envoi ou de réception, nombre de messages entrants et

sortants, de messages nettoyés, de spams, volume, format, pièces jointes, noms de domaine expéditeur de message.

Les informations relatives aux données d'identification électronique ont pour origine la DRSI et l'utilisateur (pour le mot de passe).

En ce qui concerne le destinataire, expéditeur/contact de massages, les informations relatives à l'identité et aux coordonnées proviennent de l'expéditeur.

En outre, les informations relatives à l'identité, au nom d'utilisateur, à la vie professionnelle et aux coordonnées professionnelles de l'utilisateur de la messagerie sont issues du traitement relatif à la gestion des habilitations (AD).

Enfin, les autres données sont générées par le système.

Par ailleurs, la Commission relève qu'il est indiqué dans l'annexe relative à la procédure d'enrôlement à la messagerie que : « *dans les autres cas, par téléphone, après vérification de l'identité de l'intéressé qui doit communiquer ses prénom, nom, matricule, date de naissance (procédure décrite dans le traitement « gestion des habilitations et des accès au système d'information par l'Active Directory »* ».

Toutefois, ni le présent traitement ni celui relatif à l'AD ne prévoit de collecte relative à la date de naissance des personnes concernées. En outre, la Commission relève qu'il est indiqué dans le traitement relatif à l'AD que l'inscription du matricule y est facultative. Aussi, la Commission exprime des réserves sur la maîtrise du processus d'enrôlement (notamment envoi du mot de passe O365), au niveau du quantum d'informations nominatives initialement collectées (date de naissance collectées ou non, par quel biais ? matricule présent ou non ?) qui permettent ensuite l'enrôlement à distance des personnes concernées. Aussi, les informations accessibles permettant à la DRSI de se déterminer sur la véracité de l'identité alléguée ne sont pas clairement définies.

La Commission demande donc à ce qu'un retour lui soit fait dans les meilleurs délais sur ce point.

Sous cette réserve, elle 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'un document spécifique.

Toutefois ce document n'est pas joint à la demande d'avis.

Aussi la Commission rappelle que l'information des personnes concernées doit être effectuée conformément à 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 auprès de la Direction des Réseaux et des Systèmes d'Information, ou par un accès en ligne au dossier.

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.

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

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires dans le cadre de leurs missions légalement conférées.

Les accès sont en outre définis comme suit :

- Administrateurs généraux : tout accès (sauf au contenu des messages) dans le cadre de leurs missions de gestion des comptes et de qualité du fonctionnement du service de messagerie ;

- Administrateurs de gestion des comptes: tout accès (sauf au contenu des messages) dans le cadre de leurs missions de création de comptes, d'administration des comptes et d'assistance aux utilisateurs ;

- Utilisateurs : accès en consultation, saisie et suppression selon les fonctionnalités de leurs comptes ;

- Agents habilités en cas d'absence dans le respect de la charte des systèmes d'information de l'Etat,

- Prestataires (Microsoft) : accès dans le cadre des opérations liées au fonctionnement de la solution, à l'hébergement et à la sauvegarde de la solution (sans accès aux données du client conformément à leurs engagements contractuels) ;

- Autorités habilitées : tous accès (sauf au contenu des messages) dans le respect de la règlementation applicable.

La Commission relève, eu égard aux compléments d'information qu'elle a reçus, qu'il faut entendre par autorités habilitées l'AMSN agissant dans le cadre de ses missions issues de la Loi n° 1.435 sur la criminalité technologique et de l'Ordonnance n° 5.664 du 23 décembre 2015, ainsi que « *toute autorité judiciaire, administrative ou policière habilitée en droit interne* ».

A cet égard, elle rappelle que la vie privée des utilisateurs doit être protégée, et le secret des correspondances également, conformément aux préconisations de la Commission formulées dans sa délibération n° 2015-111 du 18 novembre 2015 portant recommandation sur les traitements automatisés ou non automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique utilisée à des fins de surveillance ou de contrôle* ».

Elle rappelle ainsi avoir indiqué que « *seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des*

motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée à ses intérêts ou à la Loi. Cela peut notamment prendre la forme d'une ordonnance judiciaire mandatant un huissier de justice aux fins d'accéder, voire d'enregistrer les messages privés litigieux ».

La Commission relève toutefois qu'à l'analyse du dossier les Autorités susvisées n'ont pas accès au présent traitement mais se font communiquer des informations y relatives dans le cadre de leurs missions légalement conférées.

En ce qui concerne plus particulièrement l'AMSN, la Commission constate que cette dernière déploie des outils spécifiques de sécurité, qui permettent la collecte d'informations.

Elle considère donc qu'il s'agit d'un traitement automatisé d'informations nominatives qui doit avoir été soumis à son avis préalablement à sa mise en œuvre et à une interconnexion avec un traitement de l'Etat.

Elle rappelle à cet effet les dispositions de l'article 5 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique aux termes desquelles « *le Directeur peut mettre en œuvre des traitements (…) d'informations nominatives (…) dans le respect des dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée, susvisée* ». L'absence de précision quant au traitement déployé ne permet pas à la Commission d'apprécier la portée et les contours du contrôle opéré, et ainsi sa proportionnalité.

La Commission demande donc la suspension de l'interconnexion entre le traitement de contrôle de l'AMSN et la messagerie dont s'agit, tant qu'elle n'a pas eu à se prononcer sur le premier.

En ce qui concerne le recours à des prestataires, 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 ces derniers doivent être limités à ce qui est strictement nécessaire à l'exécution de leurs contrats de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Sous ces réserves, la Commission considère que ces accès sont justifiés.

VI. Sur les rapprochements et les interconnexions avec d'autres traitements

Le responsable de traitement indique que le traitement est rapproché avec les traitements suivants :

- Gestion des dossiers des agents et fonctionnaires de l'Etat, légalement mis en œuvre, afin « *de pouvoir identifier les agents de l'administration en activité lors de l'identification des besoins, puis les agents devant être conviés à une formation intégrant O365* »;
- Gestion du parc informatique, non légalement mis en œuvre, afin d'identifier les personnes n'ayant pas de terminal ;
- Gestion des habilitations et des accès au Système d'information par l'Active Directory, légalement mis en œuvre, afin de valider les données et leur cohérence.

Concernant le traitement ayant pour finalité « *Gestion du parc informatique*», la Commission demande à ce qu'il lui soit soumis dans les meilleurs délais.

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.

En outre, la Commission rappelle que toute copie ou extraction de données en vue de communication aux autorités judiciaires ou administratives compétentes devra être chiffrée sur son support de réception.

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

Les informations relatives à l'identité à la gestion des contacts (destinataires/expéditeurs/contacts des messages) et aux messages répondent à une politique d'archivage mise en œuvre par l'Administration.

Les informations d'identité relatives à l'administrateur (identité, vie professionnelle, coordonnées professionnelles) sont conservées jusqu'au départ de celui-ci + 30 jours. En ce qui concerne les données d'identification électronique de l'administrateur, elles sont supprimées dès son départ pour le login et à chaque renouvellement de mot de passe pour celui-ci.

Les informations d'identité relatives à l'utilisateur (identité, vie professionnelle, coordonnées professionnelles) sont conservées jusqu'au départ de celui-ci + 180 jours. En ce qui concerne les données d'identification électronique de l'administrateur, elles sont supprimées dès son départ pour le login et à chaque renouvellement de mot de passe pour celui-ci.

Les autres informations liées à la solution, qui comprennent les données de connexion, les informations temporelles et les informations en lien avec les messages, sont conservées sur une période de 12 mois glissants.

La Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Constate que les informations relatives aux adresses et coordonnées ont pour origine la DRHFPP et celles relatives à l'identification des demandeurs proviennent du traitement ayant pour finalité « *assistance aux utilisateurs* ».

Rappelle que :

- l'information des personnes concernées doit être effectuée en conformité avec 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 ;

- toute copie ou extraction de données en vue de communication aux autorités judiciaires ou administratives compétentes devra être chiffrée sur son support de réception.

Demande que :

- le traitement ayant pour finalité « *Gestion du parc informatique* » lui soit soumis dans les meilleurs délais ;

- le traitement automatisé d'informations nominatives exploité par l'AMSN aux fins de contrôler la messagerie Office 365 mise en œuvre par l'Etat lui soit soumis dans les meilleurs délais ;

- l'interconnexion entre le traitement de contrôle de l'AMSN et la messagerie dont s'agit soit suspendue tant qu'elle n'a pas eu à se prononcer sur le premier ;

- des informations supplémentaires lui soient fournies relativement à la procédure d'enrôlement des personnes concernées.

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 de la messagerie électronique professionnelle Office 365 ».***

Le Président

Guy MAGNAN