Délibération n° 2023-019 du 15 février 2023

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 et sécurisation des accès distants au Système d'Information* »

présenté par la Société Monégasque de l'Electricité et du Gaz (SMEG)

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 l'Ordonnance Souveraine n°2.578 du 13 janvier 2010 approuvant le traité de concession de la SMEG ;

Vu le traité de concession de service public de l'électricité et du gaz conclu entre la Principauté de Monaco et la SMEG entré en vigueur le 1er janvier 2009, accompagné de ses annexes et cahier des charges ;

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 Société Monégasque de l'Electricité et du Gaz (SMEG) le 24 novembre 2022 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et sécurisation des accès distants au Système d'Information* » ;

Vu la prorogation du délai d'examen de ladite demande d'avis notifiée au responsable de traitement le 23 janvier 2023, 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 15 février 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société Monégasque de l'Electricité et du Gaz (SMEG) est une société anonyme en charge de l'exploitation du service public de la distribution de l'électricité et du gaz, en application d'un traité de concession conclu avec la Principauté de Monaco, lequel est entré en vigueur le 1er janvier 2009.

Afin de permettre les accès à distance à certains environnements du système d'Information de la SMEG, de SMEG DEV et de la SMA, cette société souhaite mettre en place un dispositif de gestion et sécurisation desdits accès.

Ainsi, le traitement d'informations nominatives objet de la présente délibération 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

Ce traitement a pour finalité « *Gestion et sécurisation des accès distants au Système d'Information* ».

Les personnes concernées sont les prestataires intervenant pour le compte de la SMEG, de SMEG DEV et de la Société Monégasque d'Assainissement (SMA) ainsi que les administrateurs internes de la SMEG.

Enfin, les fonctionnalités sont les suivantes :

- permettre les accès à distance à certains environnements du Système d'Information de la SMEG, de SMEG DEV et de la SMA de manière sécurisée ;
- analyser les besoins de maintenance et communiquer avec les personnes intéressées en cas d'intervention sur le traitement (ex : maintenance) ;
- assurer la gestion d'un annuaire dédié et des comptes associés ;
- permettre la traçabilité des sessions ;
- conserver des éléments retraçant les opérations réalisées par les agents à des fins, le cas échéant, de vérification et de compréhension d'une situation donnée ;
- vérifier *a posteriori* les actions réalisées par les utilisateurs de la solution et disposer, le cas échéant, de preuves ou de débuts de preuves si besoin ;
- établir des statistiques, des rapports d'analyse sans information nominative ;
- créer des tutoriels à partir de l'enregistrement des actions réalisées.

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 traitement dont s'agit est justifié par l'exécution d'un contrat ou de mesures pré-contractuelles ainsi que par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission constate ainsi que le traitement permet « *de sécuriser les accès au SI SMEG/ SMEG DEV/SMA en encadrant les accès des prestataires* » et qu' « *il est nécessaire à l'exécution des contrats qui lient la SME ou SMEG DEV ou la SMA aux prestataires pour des opérations de tierce maintenance, dans un cadre sécurisé* ».

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.

III. Sur les informations nominatives traitées

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

- identité : nom, prénom du demandeur et des administrateurs ;
- adresses et coordonnées : email et téléphone mobile du demandeur ;
- formation, diplômes, vie professionnelle : société et fonction du demandeur, référence du contrat, application et/ou projet concerné ;
- données d'identification électronique : identifiant et mot de passe ;
- informations temporelles/horodatage : horodatage des connexions (date et heure) ;
- accès : raison de l'accès, date/heure de début, date/heure de fin, serveur, adresse IP publique depuis laquelle le/les prestataire(s) ouvre(nt) la connexion (IP de l'entreprise ou du domicile), logs de connexion sur le réseau (pare-feu/environnement/équipement interne réseau/serveur cible interne), enregistrement des sessions(vidéo des actions réalisées par la personne).

Les informations relatives à l'identité ont pour origine le contrat de prestation de service ou le contrat de travail.

Les adresses et coordonnées ainsi que les informations relatives à la formation, aux diplômes et à la vie professionnelle ont pour origine le contrat de prestation de service.

Les données d'identification électronique ont pour origine le système d'habilitations.

Les informations temporelles ont pour origine le système.

Enfin, les informations relatives aux accès ont pour origine le prestataire et 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 mention sur le document de collecte et d'un document spécifique.

L'ensemble de ces documents n'ayant pas été joint à la demande, la Commission rappelle que ceux-ci doivent impérativement comporter l'ensemble des mentions prévues 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 responsable de traitement indique que le droit d'accès s'exerce par voie postale, par courrier électronique et sur place auprès de la Direction Administrative et Juridique (DPO).

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, elle 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, la Commission 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 réserve de la prise en compte de ce qui précède, elle constate 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 et les destinataires

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

Les personnes habilitées à avoir accès au traitement sont :

- le personnel de la DSI (trois administrateurs nominativement identifiés, le RSSI et le Directeur des Systèmes d'Information) : tous droits (gestion des comptes, consultation des accès,…)

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

- ***Sur les destinataires***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités judiciaires.

La Commission estime que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, elle rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

La Commission considère donc que de telles transmissions sont conformes aux exigences légales.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement est interconnecté avec le traitement ayant pour finalité « *Gestion de l'identité et des authentifications au Système d'Information* », soumis concomitamment, ainsi qu'avec tous les traitements dont la maintenance nécessite un accès distant au serveur en interne ou par un prestataire.

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

Elle rappelle que toute interconnexion ne peut avoir lieu 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 appellent plusieurs observations.

La Commission rappelle néanmoins 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 également que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

Enfin, la Commission rappelle 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, les adresses et coordonnées, les informations relatives à la formation, aux diplômes et à la vie professionnelle ainsi que les données d'identification électronique des prestataires sont conservées le temps du contrat de prestation de service.

Les informations relatives à l'identité et les données d'identification électronique des salariés sont conservées tant que la personne est en poste.

Enfin, les informations temporelles et les informations relatives aux accès sont conservées 1 an.

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.

Rappelle que :

- les documents d'information doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;
- la réponse au droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;
- les Autorités judiciaires ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées ;
- toute interconnexion ne peut avoir lieu 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 ;

- la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

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 Société Monégasque de l'Electricité et du Gaz (SMEG) du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et sécurisation des accès distants au Système d'Information au Système d'Information* »**

Le Président

Guy MAGNAN