Délibération n° 2023-018 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 de l'identité et des authentifications 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 de l'identité et des authentifications 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 gérer les accès à son Système d'Information, cette société souhaite mettre en place un dispositif de gestion de l'identité et des authentifications.

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 de l'identité et des authentifications au Système d'Information ».*

Les personnes concernées sont les salariés de la SMEG, de SMEG DEV et de la Société Monégasque d'Assainissement (SMA) ainsi que les prestataires intervenant pour le compte de ces sociétés et les prestataires externes intervenant pour des maintenances à distance.

Enfin, les fonctionnalités sont les suivantes :

- gestion des comptes utilisateurs (création, modification, désactivation, suppression) ;
- gestion des profils et groupes utilisateurs ;
- gestion des autorisations d'accès aux ressources informatiques (création, modification, suppression) ;
- gestion de la mobilité et des départs ;
- gestion des mots de passe temporaires ;
- gestion de la sécurité des Systèmes d'Information (S.I.) : maîtrise des accès au S.I., suivi de la sécurité (anti-virus, malware), mise en place des remontées d'alertes sur les risques d'intrusion, établissement de rapports (ex : audit de sécurité, détection de risques,…) ;
- établissement de statistiques , indicateurs et tableaux de bord sans aucune donnée nominative.

La Commission constate par ailleurs à la lecture du dossier que le présent traitement a également pour fonctionnalité la gestion en toute autonomie par les utilisateurs de leur mot de passe, notamment les changements périodiques obligatoires.

Elle considère 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 « *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* ».

La Commission constate ainsi que le traitement permet « *de créer pour chaque utilisateur un compte nominatif, qui leur permet ensuite de s'authentifier* ».

Le responsable de traitement précise que « *Cette gestion centralisée des comptes permet de gérer l'accès sécurisé à l'ensemble des applications du SI SMEG/SMEG DEV/SMA* ».

Il indiqué également que « Les prestataires intervenant dans le cadre d'un contrat de tierce maintenance, doivent également se voir créer un compte » dans le présent traitement pour accéder au S.I. SMEG/SMEG DEV/SMA.

Enfin, la Commission constate à la lecture du dossier que les personnes concernées sont informées de la mise en œuvre de ce traitement et que celui-ci n'est pas mis en œuvre à des fins de surveillance.

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, date de naissance (obligatoire) ;
- adresses et coordonnées : email et numéro(s) de téléphone (obligatoire) ;
- formation, diplômes, vie professionnelle : poste, service, entreprise, hiérarchie (obligatoire si salarié), société et fonction du prestataire, référence du contrat, application et/ou projet concerné (obligatoire si prestataire) ;
- données d'identification électronique : identifiant et mot de passe, appartenance à des groupes, Token MFA ;
- informations temporelles/horodatage : horodatage des connexions (date et heure).

La Commission constate toutefois à la lecture du dossier que sont également collectées les réponses aux questions secrètes permettant aux salariés, entre autres, de réinitialiser leur mot de passe, et que ces réponses ont pour origine la personne concernée.

Les informations relatives à l'identité, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion des Ressources Humaines* » pour les salariés et le formulaire dédié pour les prestataires.

Les données d'identification électronique et les informations temporelles 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 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 (deux administrateurs nominativement identifiés, le responsable de l'équipe Infrastructure et Exploitation, le responsable DSI): droit de faire des demandes auprès du sous -traitant ;
- le sous-traitant : administration et maintenance (aucun accès en consultation de l'espace professionnel de l'utilisateur).

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 sous-traitant, 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 doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de sous-traitance. De plus, ledit sous-traitant est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

- ***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 administrative des salariés et de la paie* », en cours de modification, ainsi qu'avec tous les traitements déjà mis en œuvre et à venir dont les applicatifs ont besoin pour gérer les habilitations.

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

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, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle sont conservées 90 jours après le départ du salarié ou la fin du contrat de prestation de service.

Par ailleurs, les données d'identification électronique sont conservées le temps du contrat du travail ou du contrat de prestation de service.

Enfin, les informations temporelles sont conservées 1 an.

La Commission constate que ces durées sont conformes aux exigences légales.

Elle fixe par ailleurs la durée de conservation des réponses aux questions secrètes à la durée de l'habilitation.

Après en avoir délibéré, la Commission :

Constate que sont également collectées les réponses aux questions secrètes permettant aux salariés, entre autres, de réinitialiser leur mot de passe, et que ces réponses ont pour origine la personne concernée.

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 ;

- 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.

Fixe la durée de conservation des réponses aux questions secrètes à la durée de l'habilitation.

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 de l'identité et des authentifications au Système d'Information* ».**

Le Président

Guy MAGNAN