

Délibération n° 2024-074 du 17 avril 2024

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion des habilitations et des accès au Système d'Information de Monaco Cloud par l'Active Directory* »

présenté par Monaco Cloud S.A.M.

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'Arrêté Ministériel n° 2018-1053 du 8 novembre 2018 portant application de l'article 27 de la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

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 délibération n° 2017-206 du 20 décembre 2017 de la Commission de Contrôle des Informations Nominatives portant recommandation sur la gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au système d'information ;

Vu la demande d'autorisation déposée par Monaco Cloud S.A.M. le 21 décembre 2023 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès au Système d'Information de Monaco Cloud par l'Active Directory* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 19 février 2024, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 17 avril 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Monaco Cloud S.A.M. est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 20S08585, ayant entre autres pour objet en Principauté de Monaco « *d'assurer dans les relations intérieures et internationales, tous services de cloud computing. A ce titre : a) Elle assure la fourniture et la commercialisation de services en mode IaaS (Infrastructures as a Service), PaaS (Plateformes as a Service), ou SaaS (Software as a Service). b) En outre, elle peut : - fournir des services d'infogérance afférents à ces solutions ou des services de cloud computing et de logiciel propriétaire ou en sous-licence ; - concevoir tous services de cloud computing autres que ceux visés ci-dessus ; - créer et commercialiser tous types de solutions informatiques susceptibles d'être exploitées et distribuées dans le cadre des services de Cloud Computing ; - commercialiser et entretenir tous types d'équipements relatifs aux solutions ainsi développées ; - exercer à Monaco et à l'étranger, toutes activités qui se rattachent, directement ou indirectement, à son objet* ».

Afin de sécuriser l'accès à son système d'information (SI), cette société souhaite gérer les habilitations audit système.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance, il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Gestion des habilitations et des accès au Système d'Information de Monaco Cloud par l'Active Directory* ».

Les personnes concernées sont les collaborateurs de Monaco Cloud, les prestataires ayant accès aux SI de Monaco Cloud et les stagiaires de Monaco Cloud.

Enfin, les fonctionnalités de ce traitement 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 de la sécurité de son Système d'Information (SI) : maîtrise des accès au SI, suivi de la sécurité (antivirus, malware), mise en place de remontées d'alertes sur les risques d'intrusion, établissement de rapports (ex. détection de risques) ;
- permettre la supervision des accès aux applications (veiller à la journalisation des accès, collecter et enregistrer des événements systèmes (logs) permettant de tracer les accès des utilisateurs aux applications et données ;
- établir des rapports qui permettent de détecter des risques de malveillance et de s'assurer de la cohérence des accès avec les habilitations délivrées ;
- disposer, le cas échéant, de preuves en cas d'infractions.

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 est tout d'abord justifié par le respect d'une obligation légale, à savoir l'Arrêté Ministériel n° 2018-1053, susvisé.

Il indique par ailleurs que le traitement est également justifié par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

A cet égard, la Commission relève que « *Monaco Cloud met en œuvre ce traitement pour la sécurité et le bon fonctionnement technique du réseau et des systèmes d'information, la préservation de ses intérêts économiques, commerciaux et financiers ainsi que la prévention et la détection a priori et a posteriori de toute activité non-conforme ou illicite par des utilisateurs de ses systèmes d'information* ».

Elle prend acte enfin que « *Le présent traitement ne saurait porter atteinte aux libertés et droits fondamentaux des personnes concernées* ».

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 nominatives traitées

Les informations nominatives traitées sont :

- identité :
 - utilisateurs du SI : nom, prénom, matricule (facultatif) ;
 - gestionnaires des habilitations : nom, prénom ;
- identification du demandeur (manager) : nom, prénom ;
- adresses et coordonnées : adresse email professionnelle ;
- données d'identification électronique :
 - utilisateurs du SI : identifiant utilisateur, objet SID ;
 - gestionnaires des habilitations : identifiant utilisateur ;
- vie professionnelle (utilisateurs du SI uniquement) : lieu de travail/ des locaux de l'entreprise (Monaco), groupe d'utilisateur affecté, nom de domaine auquel l'utilisateur a accès, date d'entrée de la personne dans l'entreprise ;
- informations temporelles :
 - utilisateurs du SI : log de dernière connexion, nombre de connexions, date de création dans l'AD, date de dernière réinitialisation du mot de passe ;
 - gestionnaires des habilitations : opération réalisée (création, modification, suppression), date et heure de la dernière modification.

Le responsable de traitement indique que les informations relatives à l'identité ainsi que les adresses et coordonnées ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* ».

Les informations relatives à l'identification du demandeur ont pour origine le traitement ayant pour finalité « *Gestion du support collaborateur* ».

Les données d'identification électronique ainsi que les informations relatives à la vie professionnelle ont pour origine les gestionnaires des habilitations.

Enfin, les informations temporelles ont pour origine le système du présent traitement.

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 s'effectue par le biais d'une notice d'information que chaque collaborateur est invité à lire à son arrivée et mise sur un serveur partagé commun à tous les collaborateurs et prestataires.

Le responsable de traitement précise en outre que « *Les prestataires de Monaco Cloud sont également invités à consulter cette notice d'information dès lors qu'ils utilisent les systèmes d'information et de communication de Monaco Cloud* ».

A la lecture de l'extrait de ce document, 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, de modification et de mise à jour*

Le droit d'accès s'exerce par voie postale ou par courrier électronique auprès du Chargé de la protection des données à caractère personnel.

A cet égard, la Commission rappelle que la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, elle constate qu'une procédure a été mise en place pour permettre au responsable de traitement de s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, le responsable de traitement précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document feront 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.

La Commission considère ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

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

➤ *Sur les destinataires*

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique dans le cadre de ses missions légalement conférées.

La Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

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

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

Les personnes habilitées à accéder au traitement sont :

- les gestionnaires AD : tous droits dans le cadre de leur mission notamment de maintenance et de gestion des rôles et groupes ;
- l'équipe SSI : consultation pour les contrôles et audits sécurité.

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

La Commission rappelle par ailleurs qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet de deux rapprochements avec les traitements ayant respectivement pour finalité « *Gestion administrative des salariés* » et « *Gestion du support collaborateur* ».

Ce deuxième traitement n'ayant fait l'objet d'aucune formalité auprès d'elle, la Commission demande au responsable de traitement de le lui soumettre dans les plus brefs délais.

Elle prend acte par ailleurs que le traitement dont s'agit est interconnecté avec tous les applicatifs ayant besoin d'une habilitation pour y accéder.

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 particulière.

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 devra 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 et à la vie professionnelle ainsi que les adresses et coordonnées et les données d'identification électronique sont conservées tant que la personne est dans l'entreprise + 3 mois.

De même, les informations temporelles des utilisateurs du SI sont conservées tant que la personne est dans l'entreprise + 3 mois, à l'exception du log de la dernière connexion qui est conservé jusqu'à nouvelle connexion.

Les informations relatives à l'identification du demandeur sont conservées 12 mois.

Enfin, les informations temporelles des gestionnaires des habilitations sont conservées 12 mois glissants.

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

Elle rappelle toutefois que même si les informations peuvent être conservées 3 mois après le départ d'une personne, les habilitations de ladite personne doivent être immédiatement supprimées lors de son départ.

Après en avoir délibéré, la Commission :

Rappelle que :

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;
- la Direction de la Sûreté Publique ne peut avoir accès aux informations objet du traitement que dans le strict cadre de ses missions légalement conférées ;
- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;
- 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 devra être chiffrée sur son support de réception ;
- même si les informations peuvent être conservées 3 mois après le départ d'une personne, les habilitations de ladite personne doivent être immédiatement supprimées lors de son départ.

Demande que le traitement ayant pour finalité « *Gestion du support collaborateur* » lui soit soumis dans les plus brefs délais.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par Monaco Cloud S.A.M. du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès au Système d'Information de Monaco Cloud par l'Active Directory* ».**

Le Président

Guy MAGNAN