Délibération n° 2024-098 du 15 mai 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 accès physiques par badge magnétique* »

présenté par Monaco Cyber Sécurité

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° 2017-625 du 16 août 2017 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifié, et son annexé ;

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° 2010-43 du 15 novembre 2010 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail mis en œuvre par les personnes physiques ou morales de droit privé ;

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'autorisation déposée par Monaco Cyber Sécurité le 19 janvier 2024 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des accès physiques par badge magnétique* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 18 mars 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 15 mai 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Monaco Cyber Sécurité est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 22S09055, ayant entre autres pour objet en Principauté de Monaco « *Toutes prestations d'études, d'audit, de conseil, de formation en matière de stratégie de sécurité des organisations notamment dans les domaines logistique, informatique, électronique, cyber-sécurité, réseaux informatiques et télécommunications, ainsi que la mise en conformité des sites et installations dans le respect des réglementations en vigueur, de certification de la compétence des personnes sur les normes internationales notamment en matière d'audit, et de management de la sécurité de l'information* ».

Afin d'assurer la sécurité des biens et des personnes au sein de ses locaux, cette société souhaite installer un système de contrôle des accès par badge magnétique.

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 responsable de traitement indique que le traitement a pour finalité *« Gestion des accès physiques par badge magnétique ».*

Les personnes concernées sont les collaborateurs/alternants, les stagiaires, les prestataires de Monaco Digital et les prestataires en charge du ménage et de la sécurité.

Enfin, les fonctionnalités sont les suivantes :

- suivre l'utilisation des badges ;
- maîtriser les entrées et les sorties dans l'entreprise ;
- maîtriser l'accès à certains locaux limitativement identifiés soumis à un niveau de sécurité et faisant l'objet d'une restriction de circulation justifiée par l'activité des personnes qui y travaillent ou la protection des équipements qui y sont localisés ;
- canaliser l'accès des collaborateurs et des prestataires disposant d'un accès par badge en les autorisant à accéder aux zones d'opérations via le sas ;
- prévenir l'accès et la circulation des personnes non autorisées ou non habilitées selon les zones identifiées de l'entreprise ;
- permettre la désactivation les badges perdus ;
- permettre la constitution de preuves en cas d'infraction.

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 traitement est tout d'abord justifié par la réalisation d'un intérêt légitime poursuivi par le responsable du traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission constate ainsi que ce système va permettre de « *limiter la possibilité pour des personnes n'appartenant pas à l'entreprise de pouvoir s'y introduire, limiter les accès physiques aux environnements de travail, aux environnements où les données (personnelles ou non) sont traitées et s'assurer que les accès ne sont accordés qu'aux personnes autorisées qui ont un besoin légitime* ».

Elle prend acte en outre que ledit système « *n'a pas pour objet de surveiller les personnes ou de contrôler leur circulation sur le site* ».

Le traitement est également justifié par le respect d'une obligation légale à laquelle est soumis le responsable de traitement, notamment les règles fixées par le référentiel PASSI annexé à l'Arrêté Ministériel n° 2017-625 du 16 août 2017 et par l'Arrêté Ministériel n° 2018-1053 du 8 novembre 2018 susvisés.

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

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

- identité: nom, prénom, trigramme, nom et prénom de la personne qui a validé l'accès ;
- vie professionnelle : équipe, société, contrat, date de fin du contrat (si applicable), profil, justification de l'accès ;
- badge : numéro de badge d'accès, date de délivrance, date de suspension (avant suppression) ;
- code d'accès : code PIN associé au badge, code d'accès alarme (si autorisé) ;
- accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie ou du point de passage ;
- informations temporelles : date et heure d'entrée, date et heure de sortie pour les zones à accès restreints, date et heure de la demande d'autorisation.

La Commission prend acte que le badge attribué aux prestataires en charge du ménage et de la sécurité n'est pas un badge nominatif mais un badge délivré à l'entreprise.

Les informations relatives à l'identité et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* ».

Les informations relatives aux badge et code d'accès ont pour origine l'Administrateur SI.

Enfin, les informations relatives aux accès aux locaux et les informations temporelles ont pour origine l'outil de gestion d'accès.

La Commission constate 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***

Le responsable de traitement indique que l'information préalable des collaborateurs s'effectue par le biais d'une notice d'information qui lui est remise à sa prise de poste puis accessible sur l'Intranet de l'entreprise dans un module « *Sécurité et protection des données* ».

Lors de la mise à jour de ladite notice, un mail ou une communication sur l'Intranet sera adressé aux collaborateurs.

Les prestataires de Monaco Digital sont informés également par une notice d'information

A l'analyse de ces documents, 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.

Le responsable de traitement précise enfin que les prestataires en charge du ménage et de la sécurité seront informés par l'entreprise elle-même.

A cet égard, la Commission rappelle que l'information délivrée doit être conforme 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 courrier électronique auprès de la personne chargée 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, la Commission constate qu'une procédure a été mise en place afin de permettre au responsable de traitement de s'assurer en cas de doute que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle 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 ces conditions, la Commission constate 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 strict cadre de ses missions légalement conférées.

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

Elle considère donc que ces transmissions sont conformes aux exigences légales.

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

Les personnes habilitées à avoir accès au traitement sont :

- les administrateurs SI de Monaco Cyber Sécurité : tous droits pour la création, l'activation, la désactivation et la suppression ;
- le prestataire : tous doits dans le cadre de ses opérations de maintenance.

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 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 doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. 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 rappelle enfin 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 d'un rapprochement avec un traitement ayant pour finalité « *Gestion administrative des salariés* » et d'une interconnexion avec le traitement ayant pour finalité « *Gestion du dispositif d'alarme anti-intrusion* ».

La Commission constate que ces traitements ont été 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 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, 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.

Enfin, la Commission rappelle que toute copie ou extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

VIII. Sur les durées de conservation

Le responsable de traitement indique que les informations sont conservées tant que la personne est en poste, à l'exception des informations temporelles qui sont conservées 12 mois.

Compte tenu des justifications apportées par le responsable de traitement la Commission considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- l'information délivrée aux prestataires en charge du ménage et de la sécurité doit être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

- 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 (switch, 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 d'informations issues de ce traitement doit être chiffrée sur son support de réception.

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 Cyber Sécurité du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des accès physiques par badge magnétique* ».**

Le Président

Guy MAGNAN