

Délibération n° 2019-090 du 12 juin 2019

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 Informatique Service

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 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 Informatique Service le 10 avril 2019 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des accès physiques par badge* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 7 juin 2019, 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 12 juin 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Monaco Informatique Service est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 77S01656, ayant entre autres pour objet en Principauté de Monaco et à l'étranger « *La recherche, la mise au point, la fabrication, l'achat et la vente à l'exclusion du détail, le courtage et la commission de produits à base électro-mécanique et électronique, y compris le software* ».

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* ».

Les personnes concernées sont les salariés et prestataires.

Enfin, les fonctionnalités sont les suivantes :

- maîtriser les entrées de l'entreprise ;
- maîtriser l'accès à certains locaux limitativement identifiés comme 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 visiteurs ;
- prévenir l'accès et la circulation de personnes non autorisées ou non habilitées selon les zones identifiées de l'entreprise ;
- établir les documents nécessaires à la gestion des badges (ex. Document Excel d'attribution des badges) ;
- permettre la constitution de preuves en cas d'infraction.

La Commission rappelle toutefois que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* » aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

En l'espèce, la finalité du présent traitement doit être plus explicite c'est-à-dire être claire et précise pour les personnes concernées en indiquant que le contrôle des accès s'effectue par le biais de badges qui sont magnétiques.

Par conséquent, elle modifie la finalité comme suit : « *Gestion des accès physiques par badge magnétique* ».

II. Sur la licéité et la justification du traitement

Le traitement est 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 (nominatives ou non) sont traitées sans contrôle permanent et systématique des intéressés* ».

Le traitement est également justifié par le respect d'une obligation légale à laquelle est soumis le responsable de traitement.

A cet égard, ledit responsable de traitement précise qu'étant certifiée PASSI, « *la société doit, en outre, veiller à respecter les contraintes du référentiel (...) dans les zones répondant aux critères PASSI* ».

Il indique qu'en complément, la société doit prendre en considération les recommandations, voire les obligations fixées notamment par le référentiel PASSI (annexe à l'Arrêté Ministériel n°2017-625 du 16 août 2017) concernant la sécurité des locaux des prestataires d'audit de la sécurité des systèmes d'information (PASSI), par la politique de sécurité des systèmes d'information de l'Etat (Arrêté Ministériel 2017-56 du 1^{er} février 2017) et par les annexes à 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.

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 (trois premières lettres du nom) ;
- vie professionnelle : centre de service, fonction ;
- informations temporelles : date et heure d'entrée, date et heure de sortie pour les zones à accès restreints ;
- accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie, ou du point de passage ;
- données d'identification: code d'accès (associé au badge), numéro de badge ou de la carte d'accès, date de délivrance, date de validité/d'expiration ;
- log de connexion administrateur : IP, données d'horodatage, identifiant de l'administrateur.

Les informations relatives à l'identité et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* » pour les salariés et le responsable du centre où la personne est affectée pour les prestataires.

Les informations relatives aux informations temporelles et aux accès aux locaux ont pour origine l'outil de gestion des accès.

Les informations relatives aux données d'identification ont pour origine le Directeur des Systèmes d'Information (DSI).

Enfin, les logs de connexion administrateur 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*

Le responsable de traitement indique que l'information préalable s'effectue par le biais d'un document spécifique et d'un affichage.

Ces documents n'ayant pas été joints à la demande d'autorisation, la Commission rappelle, conformément à sa délibération n° 2010-43 du 15 novembre 2010 que l'information préalable des personnes concernées doit 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 droit d'accès s'exerce par voie postale.

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*

Les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique.

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 gestionnaires des badges (DSI, PASSI, RH) : création, modification, suppression des badges sachant que le DSI et la RH ont tous les droits à l'exception de la zone « *PASSI* » ;
- le personnel habilité « *PASSI* » pour cette même zone : tout accès ;
- les administrateurs de l'outil (DSI et PASSI) : tout accès (pour la zone PASSI, la RH n'a pas d'accès) ;
- le personnel habilité du prestataire du contrôle d'accès : tous accès, sauf la zone PASSI.

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

La Commission rappelle toutefois 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* ».

La Commission constate que ledit traitement a 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 demande que toute copie ou extraction d'informations issues de ce traitement soit chiffrée sur son support de réception.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations relatives à l'identité, à la vie professionnelle et aux données d'identification électronique sont conservées tant que la personne travaille dans l'entreprise pour les salariés et la durée de contrat ou de la prestation de service pour les prestataires.

Par ailleurs, il précise que les informations temporelles, les accès aux locaux et les logs de connexion sont conservés 12 mois conformément à ses obligations réglementaires.

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

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion des accès physiques par badge magnétique* ».

Constata que toute copie ou extraction d'informations issues de ce traitement sera chiffrée sur son support de réception.

Rappelle que :

- l'information préalable des personnes concernées doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;
- les Services de Police monégasque ne pourront avoir communication des informations objet du traitement que dans le strict cadre de leurs 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 (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.

Demande que toute copie ou extraction d'informations issues de ce traitement soit 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 Informatique Service du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des accès physiques par badge magnétique* ».**

Le Président

Guy MAGNAN