

Délibération n° 2020-158 du 18 novembre 2020

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

« *Contrôle d'accès aux locaux par badge non biométrique* »

présenté par Edmond de Rothschild (Monaco)

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 Edmond de Rothschild (Monaco) le 31 juillet 2020 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Sécurité et contrôle d'accès sur le lieu de travail* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 29 septembre 2020, 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 18 novembre 2020 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Edmond de Rothschild (Monaco) est une société établie à Monaco sous le numéro de RCI 92S02760, ayant notamment pour activité « *Tant en Principauté de Monaco qu'à l'étranger, pour son compte ou le compte de tiers directement ou en participation : -d'effectuer toutes opérations de banque, de crédit d'escompte, de prêt d'avance, de commission, de courtage, de change, d'arbitrage, (...)* ».

Afin d'assurer la sécurité des biens et des personnes au sein de ses locaux, cette société souhaite mettre en place un dispositif de contrôle d'accès par badge.

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 ce traitement a pour finalité « *Sécurité et contrôle d'accès sur le lieu de travail* ».

Il précise que les personnes concernées sont les employés et les tiers. A cet égard, la Commission constate, à la lecture du dossier, que les tiers sont les auditeurs externes et les prestataires/sous-traitants permanents.

Enfin, les fonctionnalités sont les suivantes :

- assurer la sécurité des biens et des personnes par ségrégation des accès entre les clients, le personnel et les intervenants extérieurs ;
- assurer la sécurité des personnes et des biens en contrôlant les accès aux locaux identifiés comme sensibles bénéficiant d'une circulation limitée ;
- gérer les habilitations d'accès aux personnes autorisées ;
- désactiver les badges perdus/volés ;
- permettre la constitution de preuves en cas d'infractions.

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 dispositif mis en place a pour but de contrôler les accès aux locaux par le biais de badge non biométrique.

Par conséquent, elle modifie la finalité comme suit : « *Contrôle d'accès aux locaux par badge non biométrique* ».

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que 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.

A cet égard, la Commission constate que le dispositif va permettre d'assurer « *la protection des personnes et des biens ainsi qu'assurer la confidentialité des données détenues grâce à une restriction d'accès aux locaux aux seules personnes dûment habilitées* ».

Le responsable de traitement précise par ailleurs que « *Le traitement n'a pas pour objet de contrôler de manière inopportune les comportements, les habitudes et les horaires des personnes concernées par le traitement* ».

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, numéro d'employé pour les employés, nom et prénom pour les auditeurs externes et les prestataires/sous-traitants permanents ;
- formation, diplômes, vie professionnelle : service, plages horaires habituellement autorisées, zone d'accès autorisée ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux informations et au traitement ;
- informations temporelles : date et heure de passage à une zone, nom et/ou numéro du point de passage ;
- badges : numéro de badge.

Les informations relatives à l'identité, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* » pour les employés et les contrats ou lettres de mission avec les auditeurs externes et les prestataires/sous-traitants permanents.

Les données d'identification électronique, les informations temporelles et le numéro de badge ont pour origine le système de contrôle d'accès par badge.

La Commission considère 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 employés se fait tout d'abord par une procédure interne accessible en intranet, à savoir une directive interne.

A la lecture de ce document, la Commission constate que ladite procédure est en réalité un document d'ordre général qui décrit le processus de déclaration des traitements automatisés de données personnelles ainsi que les conditions dans lesquelles s'exerce le droit d'accès aux informations au sein d'Edmond de Rothschild (Monaco).

Elle relève toutefois que l'information des employés et des tiers se fait également par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé.

Aussi, à la lecture du formulaire de délivrance de badge joint à la demande, 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 sur place auprès du Chief Operating Officer.

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 aux Autorités policières ou judiciaires légalement habilitées.

La Commission estime ainsi que la communication aux Autorités policières ou judiciaires peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, lesdites Autorités ne pourront avoir communication des informations que dans le strict cadre de leurs 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 avoir accès au traitement sont :

- les membres des Services Généraux et Sécurité : inscription, modification, mise à jour et consultation ;
- le prestataire : tous droits dans le cadre de ses opérations de maintenance du système, uniquement sous la supervision d'un personnel de la banque habilité.

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 constate 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 est 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'une interconnexion avec le traitement ayant pour finalité « *Gestion administrative des salariés* ».

La Commission constate que ce 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) 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 que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception, conformément à la délibération n° 2010-43 du 15 novembre 2010.

La Commission 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.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations relatives à l'identité, à la formation, aux diplômes et à la vie professionnelle ainsi qu'aux badges sont conservées 5 ans après la fin du contrat de travail pour les employés ou 5 ans après la fin de la mission pour les auditeurs et prestataires/sous-traitants permanents.

Les logs de connexion sont conservés 1 an.

Enfin, les informations temporelles sont conservées 6 mois après le passage.

Concernant les informations temporelles, la Commission rappelle toutefois que, conformément à sa délibération n°2010-43 du 15 novembre 2010, celles-ci ne doivent pas être conservées au-delà d'une durée de trois mois.

De même, elle considère que les données concernant les auditeurs et prestataires/sous-traitants permanents ne doivent pas être conservées au-delà d'une durée de trois mois à compter de la fin de leur mission.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Contrôle d'accès aux locaux par badge non biométrique* ».

Rappelle que :

- les Autorités policières ou judiciaires 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 tenue à jour doit lui être communiquée à première réquisition ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs) 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 informations temporelles à trois mois maximum et celle des données concernant les auditeurs et prestataires/sous-traitants à trois mois maximum à compter de la fin de leur mission.

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 Edmond de Rothschild (Monaco) du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle d'accès aux locaux par badge non biométrique* ».**

Le Président

Guy MAGNAN