

Délibération n° 2017-097 du 21 juin 2017

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

« *Sécurité et contrôle d'accès sur le lieu de travail* »

présenté par Crédit du Nord – Succursale de 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 Crédit du Nord – Succursale de Monaco le 4 avril 2017 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 1^{er} juin 2017, 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 21 juin 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Banque Crédit du Nord dont le siège social est sis à Lille en France dispose d'une succursale à Monaco où elle est valablement immatriculée au registre du Commerce et de l'industrie sous le numéro 66S01153

Afin d'assurer la sécurité des biens et des personnes ainsi que la confidentialité des données détenues, le responsable de traitement souhaite procéder à l'installation d'un système de contrôle d'accès par badge non biométrique au sein de son établissement.

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

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

Les personnes concernées sont les employés, les auditeurs externes, prestataires, sous-traitants permanents.

Enfin, les fonctionnalités sont les suivantes :

- « *Assurer la sécurité des personnes et des biens par ségrégation des accès entre les clients et 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 preuve 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

Dans le cadre de ses activités, l'établissement Crédit du Nord – Succursale de Monaco est amené à exploiter des données pour le compte de ses clients, et notamment des données relatives aux activités bancaires.

A cet égard, le responsable de traitement indique que le traitement est justifié par la réalisation d'un intérêt légitime car il permet 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* ».

La Commission note que « *Crédit du Nord Succursale de Monaco ne méconnaît pas pour autant les libertés et droits fondamentaux des personnes concernées. 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* ».

Au vu de ce qui précède, la Commission considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité : employés/ tiers (auditeurs externes, prestataires, sous-traitants permanents) : nom, prénom ;
- formation - diplômes - vie professionnelle : fonction, service, plages horaires habituellement autorisées, zones d'accès autorisées ;
- données d'identification électronique : logs de connexion des personnels habilités à avoir accès aux informations et au traitement ;
- horodatage des accès aux locaux : date et heure de passage à une zone à accès restreint, nom et/ou numéro de la porte d'entrée/ sortie, ou du point de passage ;
- badge : numéro de badge, date de délivrance, état (activé ou désactivé), date de validité.

Les informations relatives à l'identité, la formation - les diplômes - la vie professionnelle concernant les salariés, trouvent leur origine dans le traitement légalement mis en œuvre « *Gestion administrative des salariés* » et s'agissant des auditeurs externes, des prestataires permanents et sous-traitants, lesdites informations trouvent leur origine au sein des contrats ou des lettres de mission les liant au responsable de traitement.

Les informations relatives aux données d'identification électronique, à l'horodatage des accès aux locaux, et aux badges sont générées par le système lui-même.

Au vu de ce qui précède, la Commission considère que les informations traitées 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***

La Commission note que l'information préalable des personnes concernées est effectuée comme suit :

- pour les salariés, par le biais du Règlement Intérieur et au moyen d'une note de service « *Traitement automatisés d'informations nominatives* » accessible à l'ensemble des collaborateurs sur l'intranet de la banque ;

Elle relève après analyse du dossier, que l'information préalable des salariés s'effectue également par le biais du formulaire de délivrance de badge.

- pour les tiers soit, les auditeurs externes, prestataires, sous-traitants permanents, par le biais du formulaire de délivrance de badge.

La Commission considère, à la lecture des documents qui ont été joints, qu'ils ne comportent pas l'ensemble des mentions prévues par l'article 14 de la Loi n°1.165 du 23 décembre 1993.

En conséquence, elle demande que l'information préalable des personnes concernées soit assurée conformément 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 sur place. La réponse à ce droit d'accès s'exerce selon les mêmes modalités.

Le délai de réponse à une demande de droit d'accès est de 30 jours.

La Commission constate 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 et Judiciaires Monégasques légalement habilitées.

La Commission estime que la communication auxdites Autorités peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, les Autorités susmentionnées 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 :

- le Directeur Administratif : en consultation, modification, inscription, mise à jour;
- le prestataire externe : en maintenance sous le contrôle du directeur Administratif ;
- les agents de la Sûreté publique : dans le cadre de leur mission.

S'agissant des agents de la Sûreté Publique, la Commission considère qu'ils sont uniquement destinataires des informations et qu'ils n'ont pas d'accès direct et permanent au traitement.

A la condition de la prise en compte de ce qui précède, les accès susvisés sont justifiés.

En ce qui concerne le prestataire, elle 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* » 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 relève néanmoins que les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Par ailleurs, elle constate que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception, conformément à la délibération n° 2010-13 du 3 mai 2010.

Enfin, 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

Les informations relatives à l'identité, la formation - les diplômes - la vie professionnelle et les badges sont conservées 5 ans après la fin du contrat de travail pour les employés et 5 ans après la fin de mission pour les auditeurs externes, prestataires ou sous-traitants permanents.

Les informations relatives aux données d'identification électronique sont conservées un an à partir de la connexion.

Les informations relatives à l'horodatage des accès sont conservées 3 mois après le passage.

La Commission considère que cette durée est conforme aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- 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) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Considère que les agents de la Sûreté Publique sont uniquement destinataires des informations et qu'ils ne pourront en avoir communication que dans le strict cadre de leurs missions légalement conférées.

Constate que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

Demande que l'information préalable des personnes concernées comporte l'ensemble des mentions prévues par l'article 14 de la Loi n°1.165 du 23 décembre 1993.

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 Crédit du Nord – Succursale de Monaco du traitement automatisé d'informations nominatives ayant pour finalité « Sécurité et contrôle d'accès sur le lieu de travail ».**

Le Président

Guy MAGNAN