Délibération n° 2017-100 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

« *Gestion et traçabilité des habilitations informatiques* »

présenté par la Compagnie Monégasque de Banque

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 Recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° 1.338 du 7 septembre sur les activités financières, modifiée ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007, modifiée, portant application de la Loi n° 1.338 du 7 septembre 2007, modifiée, susvisée ;

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 français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution ;

Vu la demande d'autorisation déposée par la Compagnie Monégasque de Banque, le 7 mars 2017, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Gestion et traçabilité des habilitations informatiques* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 5 mai 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 Compagnie Monégasque de Banque une société anonyme monégasque immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 76S01557, qui a pour objet *« de faire dans la Principauté de Monaco (….) toutes opérations bancaires et financières (…)».*

Dans le cadre de son organisation interne, et afin d'assurer la sécurité informatique de son réseau, la Compagnie Monégasque de Banque souhaite mettre en œuvre un traitement ayant pour finalité « *Gestion et traçabilité des habilitations informatiques* ».

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 soumis a pour finalité « *Gestion et traçabilité des habilitations informatiques* ».

Il concerne les employés et les prestataires de la banque.

Le responsable de traitement indique que les fonctionnalités sont les suivantes :

- « *Créer et gérer des profils utilisateurs en fonction notamment des mobilités internes et départs ;*
- *Contrôler la séparation des tâches en fonction des divers profils utilisateurs et des fonctions de chacun au sein de la société ;*
- *Administrer les droits d'accès aux applications et aux dossiers hébergés sur les serveurs ;*
- *Protéger les intérêts économiques, commerciaux et financiers de la banque auxquels est attaché un caractère de confidentialité et lutter contre les pratiques contraires (concurrence déloyale, divulgation de données confidentielles de la société, violation du secret bancaire ou de secrets d'affaires de la société) ;*
- *Procéder à des contrôles afin de s'assurer de la conformité des droits délivrés par rapport aux règles édictées en matière d'accès à l'information ;*
- *Collecter des évènements systèmes permettant de tracer les habilitations octroyées, visant à prévenir le risque de fraude et de s'assurer de la cohérence des accès ;*
- *La détection éventuelle de comportements anormaux ;*
- *L'établissement de reportings à usage interne ;*
- *L'interconnexion avec l'ensemble des traitements nécessitant des habilitations*».

La Commission constate que la finalité du traitement est explicite et légitime, conformément à 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 justifié par le respect d'une obligation légale à laquelle est soumis le responsable de traitement ainsi que par la réalisation d'un intérêt légitime, sans que soient méconnus ni l'intérêt, ni les libertés et droits fondamentaux des personnes concernées.

A cet égard, il indique que le présent traitement « *participe à la sécurisation du système informatique de la banque conformément aux exigences des articles 17 et 17-1 de la Loi n°1.165 du 13 décembre 1993* » et précise que l'article 11 du titre II de l'Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque soumises au contrôle de l'ACPR, prévoit l'obligation de « *vérifier les conditions d'évaluation, d'enregistrement, de conservation et de disponibilité de l'information, notamment en garantissant l'existence de la piste d'audit au sens de l'article 85 et de vérifier la qualité des systèmes d'information et de communication* », ainsi que l'article 6 de l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 relatif aux mécanismes de sécurité et de contrôle internes qui contient des dispositions équivalentes.

Par ailleurs, il indique que le traitement est également justifié par la réalisation d'un intérêt légitime destiné à *« protéger les intérêts économiques, commerciaux et financiers de la banque auxquels est attaché un caractère de confidentialité et lutter contre les pratiques contraires (concurrence déloyale, divulgation de données confidentielles de la société, violation du secret bancaire ou de secrets d'affaires de la société)* » et à permettre la « *détection éventuelle de comportements anormaux* ».

La Commission en prend acte.

Aussi, elle considère que ce traitement est licite et justifié, au sens des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : nom, prénom ;
- formation - diplôme – vie professionnelle : fonction du salarié ;
- données d'identification électronique : identifiant numérique, mot de passe, applications et profils associés ;
- traçabilité : horodatage, outil informatique utilisé, traces d'exécution.

Les informations relatives à l'identité et à la formation, les diplômes, la vie professionnelle, ont pour origine le dossier du personnel.

Les données d'identification électronique sont élaborées par le Service IT.

Enfin, la traçabilité est générée automatiquement par le système.

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 personnes concernées est assurée par une procédure interne accessible en Intranet.

Toutefois, le document susvisé n'étant pas joint à la présente demande, la Commission n'est pas en mesure de vérifier si la qualité de l'information dispensée est conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Aussi elle rappelle que l'information préalable de l'ensemble des personnes concernées doit être assurée conformément à l'article 14 de la Loi susvisée.

- ***Sur l'exercice du droit d'accès, de modification et de mise à jour :***

L'exercice du droit d'accès s'effectue par courrier électronique.

La Commission rappelle que le délai de réponse doit s'effectuer dans le mois suivant la demande.

La Commission considère donc 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 personnes ayant accès au traitement et les communications d'informations

- ***Sur les accès au traitement***

Le responsable de traitement indique qu'ont accès au traitement :

- le département informatique : en inscription, modification, mise à jour et consultation ;
- le département Contrôle Périodique Risk Management : en consultation ;
- le département Audit : en consultation ;
- les prestataires habilités dans le cadre des prestations de service dont ils ont la charge sur place en présence de l'un des membres du département informatique.

En ce qui concerne les prestataires, 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 leur contrat de prestation de service. De plus, lesdits prestataires sont 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 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.

- ***Sur les communications d'informations***

Le responsable de traitement déclare que des informations peuvent être communiquées aux Autorités Policières et Judicaires légalement habilitées dans le cadre de leurs missions légalement conférées.

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, ces Autorités ne pourront avoir communication des informations objet du traitement, que dans le strict cadre de leurs misions légalement conférées.

Elle considère que de telles transmissions sont conformes aux exigences légales.

VI. Sur les rapprochements et les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement est interconnecté avec l'ensemble des traitements automatisés de l'établissement.

La Commission estime que le présent traitement pourra également être interconnecté à tous traitements futurs de la Compagnie Monégasque de Banque à des fins de sécurité.

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.

Cependant, 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.

La Commission rappelle de plus que, conformément à l'article 17 de la Loi n° 1.165, modifiée, 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 nominatives relatives à l'identité sont conservées trois mois après le départ du salarié.

Les informations relatives à la formation, la vie professionnelle, les diplômes et aux données d'identification électronique sont conservées jusqu'au départ du salarié.

Les informations relatives à la traçabilité sont conservées une année glissante.

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

Après en avoir délibéré, la Commission :

Constate que le présent traitement pourra être interconnecté avec tous les traitements futurs de la Compagnie Monégasque de Banque si cela est nécessaire à des fins de sécurité.

Rappelle que :

- l'information préalable de l'ensemble des personnes concernées doit être assurée conformément à l'article 14 de la Loi n° 1.165 ;

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

Sous réserve de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par la Compagnie Monégasque de Banque du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et traçabilité des habilitations informatiques ».***

Le Président

Guy MAGNAN