Délibération n° 2017-068 du 19 avril 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 des habilitations et traçabilité des accès aux systèmes d'informations*»

présenté par Andbank Monaco SAM

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne 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° 1.284 du 10 septembre 2007, modifiée, portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, 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 soumises au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution ;

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 demande d'autorisation déposée par Andbank Monaco SAM le 18 janvier 2016 concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité «*Gestion des habilitations et traçabilité des accès aux systèmes d'informations* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 16 mars 2017, conformément à l'article 11.1 de la Loi n°1.165, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 19 avril 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Andbank Monaco SAM est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 07S04639, qui a notamment pour objet social « *en Principauté de Monaco et à l'étranger, pour son compte ou pour le compte de tiers, directement ou indirectement ou en participation : la réalisation de toutes opérations de banque ou connexe telles que définies par la loi bancaire applicable ; la gestion de portefeuilles de valeurs mobilières, d'instruments financiers à terme ; la transmission d'ordres sur les marchés financiers, portant sur des valeurs mobilières, des instruments financiers à terme ; l'activité de conseil et d'assistance liée à ces activités (…)* ».

Dans le cadre de son organisation interne, et afin d'assurer la sécurité informatique de son réseau, elle souhaite mettre en place un système d'habilitations et de traçabilité des accès aux systèmes d'informations.

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 a pour finalité « *Gestion des habilitations et traçabilité des accès aux systèmes d'informations* ».

Les personnes concernées sont le *« personnel salarié ».*

Enfin, les fonctionnalités du traitement sont :

- la création et la gestion des profils utilisateurs (Création, activation, mise à jour, suppression) ;
- l'octroi et la gestion des droits d'accès aux différentes solutions informatiques utilisées par le responsable de traitement dans le cadre de son activité ;
- l'octroi et la gestion des droits d'accès aux dossiers et aux informations qu'ils contiennent ;
- la protection de la confidentialité de certaines informations économiques, commerciales et financières du responsable de traitement et de sa clientèle ;
- la sécurité et le bon fonctionnement des systèmes informatiques déployés par le responsable de traitement.

La Commission considère 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 responsable de traitement indique que le présent traitement est justifié par le respect d'une obligation légale.

La Commission relève ainsi que l'article 6 de l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 imposent aux établissements bancaires et assimilés de « *disposer d'une organisation administrative et comptable, ainsi que des mécanismes de sécurité et de contrôle interne et externe adéquats, notamment en ce qui concerne les opérations pour compte propre et les opérations personnelles de leurs salariés* ».

Par ailleurs, l'article 11 du titre II de l'Arrêté du 3 novembre 2014 dispose que « *le système de contrôle des opérations et des procédures internes a notamment pour objet, dans des conditions optimales de sécurité, de fiabilité et d'exhaustivité, de (…e) vérifier la qualité des systèmes d'information et de communication (…)* ».

Le responsable de traitement indique en outre que ledit traitement est également justifié par la réalisation d'un intérêt légitime.

La Commission constate ainsi que ce traitement « *permet de garantir la sécurité des systèmes d'informations et de limiter l'accès aux informations confidentielles détenues par le Responsable de Traitement, de manière à en assurer la disponibilité, l'intégrité et la confidentialité* ».

Elle note enfin qu'il permet « *de limiter les risques de fraude, de violation du secret professionnel, de fuite de données confidentielles,…* » et que la traçabilité des accès permet « *de vérifier l'identité des Utilisateurs à l'origine d'une opération lorsqu'une éventuelle activité illicite est détectée* ».

A cet égard, le responsable de traitement précise que le traitement « *n'a pas pour objectif la surveillance continue des salariés et a pour fonction de s'assurer que les droits d'accès délivrés aux salariés sont conformes à leurs fonctions* ».

La Commission considère donc que le 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 exploitées aux fins du présent traitement sont :

- identité : nom et prénom du collaborateur concerné ;
- formation-diplômes-vie professionnelle : fonction de la personne concernée (poste de travail) et Service auquel elle est affectée ;
- données d'identification électronique : identifiant et mot de passe, habilitations ;
- traçabilité : identifiants de connexion, connexion active ou non-active, date et heure de l'accès, nature de l'action effectuée par le collaborateur concerné.

Les informations relatives à l'identité, à la formation, aux diplômes et à la vie professionnelle ont pour origine le département RH.

Les informations relatives aux donnés d'identification électronique ont pour origine à la fois le département RH (habilitations) et le responsable informatique (login et mot de passe).

A cet égard, la Commission prend acte que ce mot de passe sera ensuite modifié par la personne concernée.

Enfin, les informations relatives à la traçabilité sont générées par la solution IT concernée.

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 des personnes concernées***

Le responsable de traitement indique que l'information préalable est effectuée par le biais d'une mention ou clause particulière intégrée dans chaque contrat de travail, et par un affichage.

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.

- ***Sur l'exercice du droit d'accès des personnes concernées***

Le droit d'accès s'exerce par voie postale, par courrier électronique ou sur place auprès du Responsable des Ressources Humaines.

La réponse à ce droit d'accès s'exerce selon les mêmes modalités.

Le délai de réponse est de 30 jours.

La Commission considère 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 des informations sont susceptibles d'être communiquées aux Autorités judiciaires légalement habilitées « *dans le cas où une activité illicite serait détectée et des poursuites engagées* ».

La Commission constate ainsi que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête. A cet égard, elle rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

La Commission considère donc que de telles transmissions sont conformes aux exigences légales.

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

Les personnes ayant accès au traitement sont :

- les collaborateurs du Service Informatique du responsable de traitement et de sa maison mère à Andorre : en inscription, modification, mise à jour, consultation et suppression ;
- le Secrétaire Général de l'établissement : en consultation uniquement, dans l'hypothèse où une activité illicite serait détectée ;
- le Directeur des Risques : en mode consultation uniquement, dans l'hypothèse où une activité illicite serait détectée ;
- le prestataire : tous droits 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, ses droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, celui-ci est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Elle 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 rapprochements et les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement est interconnecté avec une liste détaillée de 14 traitements légalement mis en œuvre ou concomitamment soumis.

A cet égard, la Commission constate que le traitement est également interconnecté avec le traitement « *Gestion des obligations légales aux échanges automatiques d'informations à des fins fiscales* », légalement mis en œuvre.

Le responsable de traitement précise par ailleurs qu'il est interconnecté avec deux autres traitements relatifs aux listes SICCFIN et à la messagerie électronique.

Ces deux traitements n'ayant fait l'objet d'aucune formalité auprès de la CCIN, la Commission demande au responsable de traitement de les lui soumettre dans les plus brefs délais.

Elle estime enfin que le présent traitement pourra également être interconnecté à tous traitements futurs mis en place par le responsable de traitement 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.

Elle rappelle de plus 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, à la formation, aux diplômes et à la vie professionnelle sont conservées 3 mois après le départ du salarié concerné.

Les informations relatives aux données d'identification électronique sont conservées pendant toute la durée de la relation contractuelle entre la banque et le salarié.

Enfin, les informations relatives à la traçabilité sont conservées un an à compter de leur collecte.

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

Après en avoir délibéré, la Commission :

Estime que le présent traitement pourra être interconnecté avec tous les traitements futurs du responsable de traitement si cela est nécessaire à des fins de sécurité.

Constate que la liste nominative des personnes ayant accès au traitement est tenue à jour et précise qu'elle doit lui être communiquée à première réquisition.

Rappelle que :

- les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées ;

- 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.

Demande que le responsable de traitement lui soumette dans les plus brefs délais les traitements relatifs aux listes SICCFIN et à la messagerie électronique.

A la condition de la prise en compte des éléments qui précèdent,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par Andbank Monaco SAM du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations et traçabilité des accès aux systèmes d'informations* ».**

Le Président

Guy MAGNAN