DELIBERATION N° 2016-73 DU 15 JUIN 2016 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION A LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *GESTION DES HABILITATIONS ET DES ACCES AVEC TRAÇABILITE* » PRESENTE PAR LA SUCCURSALE CREDIT AGRICOLE MONACO

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 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 la Loi n° 1.338 du 7 septembre sur les activités financières, 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 l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, 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 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 la Caisse Régionale de Crédit Agricole Mutuel Provence Côte d'Azur, le 15 mars 2016, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Gestion des habilitations et des accès avec traçabilité* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 13 mai 2016, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 15 juin 2016 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Caisse Régionale de Crédit Agricole Mutuel Provence Côte d'Azur (Alpes de Haute Provence – Alpes Maritime – Var), disposant à Monaco d'une succursale, est immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 89S02490, et a pour activité « *toutes opérations que peut accomplir un établissement de crédit dans le cadre de la règlementation bancaire et conformément aux dispositions régissant le Crédit Agricole Mutuel* ».

Afin d'accomplir ses formalités légales, elle s'est faite représenter à Monaco par sa succursale. Aussi, rappelant sa prise de position lors de la séance plénière du 24 février 2016 aux termes de laquelle la Commission a estimé que seuls les responsables de traitements qui n'étaient pas établis à Monaco devaient choisir un représentant établi à Monaco, elle constate que le responsable de traitement est établi en Principauté par le biais de sa succursale.

C'est donc cette dernière qui soumet le présent traitement.

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

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 des habilitations et des accès avec traçabilité* ».

Il concerne les « *collaborateurs* » de la succursale de Monaco. A cet égard, le responsable de traitement précise que « *le terme « collaborateurs » désigne seulement les employés de la banque* ».

Les fonctionnalités sont les suivantes :

- « *créer et gérer des profils utilisateurs ;*
- *administrer les droits d'accès aux applications et aux dossiers hébergés sur les serveurs de la succursale ;*
- *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) ;*
- *assurer la sécurité et/ou le bon fonctionnement des systèmes informatiques de la société ainsi que la protection physique des installations de la banque (notamment contre les phénomènes de saturation ou d'engorgement, la propagation de virus, etc.) ;*
- *fiabilisation périodique des habilitations ;*
- *interconnexion avec l'ensemble des traitements nécessitant des habilitations* ».

Par ailleurs, le responsable de traitement précise que « *dans le cas où une éventuelle activité illicite serait détectée, la traçabilité permet de retrouver l'origine des opérations* ».

Aussi, la Commission constate à la lecture du dossier et de ses annexes, que le traitement a également pour fonctionnalités :

- la collecte des évènements systèmes afin de tracer les accès des utilisateurs aux applications et aux données ;
- l'établissement de reportings.

Aussi, elle considère que la finalité du traitement est déterminée, 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 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 précise que si « *les habilitations (…) sont un moyen d'assurer la sécurité du système informatique* » et que dans l'hypothèse où « *une éventuelle activité illicite serait détectée, la traçabilité permet de retrouver l'origine des opérations* », « *le traitement n'a pas pour objectif la surveillance continue des salariés et a pour fonction de s'assurer que les droits octroyés aux collaborateurs sont compatibles avec leur fonction* ».

Il indique en outre que « *tous les agents de la succursale du CA de Monaco ont connaissance des procédures et accès à celles-ci* », qu'une charte informatique est mise à disposition des collaborateurs dans l'intranet et qu'une formation à la sécurité logique est au catalogue des formations internes du GIE Crédit Agricole Technologies auquel le responsable de traitement a adhéré et qui est en charge de la gestion des ressources et des moyens informatiques de l'ensemble des Caisses régionales du Groupe Crédit Agricole.

Par ailleurs, la Commission relève que le traitement dont s'agit participe à la vérification de la qualité des systèmes d'information conformément aux exigences de 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, et contribue aux mécanismes de sécurité et de contrôle interne conformément aux exigences de l'article 6 de l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007.

Aussi, elle considère 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 nominatives traitées sont :

- identité : nom, prénom ;
- données d'identification électronique : matricule, mot de passe, profil ;
- traçabilité : identifiant de l'employé, code transaction, version du logiciel, code retour (oui/non – transaction autorisée ou non), date et heure de l'accès, nom de l'employé, nom de la transaction.

Les informations relatives à l'identité ont pour origine le collaborateur, les données d'identification électroniques proviennent du Service Sécurité logique de Crédit Agricole Saint Laurent du Var (France) et la traçabilité est issue du système lui-même.

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 au moyen d'une procédure interne accessible en intranet.

A l'examen du document intitulé « *Gestion du personnel Crédit Agricole Provence Côte d'Azur – Gestion spécifique à la succursale de Monaco* » et notamment à la partie consacrée à « *l'information des agents de la succursale de Monaco* », la Commission estime que l'information des personnes concernées est conforme 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***

Les droits d'accès, de modification, de mise à jour et de suppression s'exercent par courrier électronique ou sur place, auprès du responsable des opérations, du directeur de la succursale de Crédit Agricole de Monaco ou son adjoint. 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 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 :

- en consultation : les services audit du Crédit Agricole Provence Côte d'Azur (siège de Saint Laurent du Var) et de Crédit Agricole S.A. (siège social à Paris) ;

- en consultation, inscription, modification et mise à jour : le service sécurité logique et le RSSI du Crédit Agricole Provence Côte d'Azur (siège de Saint Laurent du Var) et l'administrateur des habilitations de Crédit Agricole Technologies et Services (entité du groupe localisée à Montpellier).

A cet égard, la Commission rappelle que conformément à l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993, le responsable de traitement est tenu de « *déterminer nominativement la liste des personnes qui ont seules accès, pour les stricts besoins de l'accomplissement de leurs missions, aux locaux et aux installations utilisées pour les traitements, de même qu'aux informations traitées* ».

Aussi, elle considère que ces accès sont justifiés.

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

Le responsable de traitement déclare que des informations peuvent 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.

Elle rappelle par ailleurs qu'elles sont susceptibles d'être communiquées aux Autorités compétentes dans le cadre des missions qui leurs sont légalement conférées.

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 8 autres traitements légalement mis en œuvre ou concomitamment soumis.

Aussi, la Commission estime que le présent traitement pourra également être interconnecté, à des fins de sécurité, avec les futurs traitements mis en œuvre par le responsable de traitement.

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.

La Commission relève néanmoins que l'architecture technique repose sur des équipements de raccordements (switchs, routeurs, pare-feux) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés.

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

Le responsable de traitement indique que les informations nominatives collectées sont conservées « *la durée de vie contrat* », à l'exception de celles relatives à la traçabilité qui le sont pour une durée de 1 an.

La Commission considère que ces durées de conservation ne sont pas en adéquation avec la finalité du traitement et les fixe en conséquence ainsi que suit :

- s'agissant de l'identité : 3 mois après le départ du collaborateur ;
- s'agissant des données d'identification électronique : la durée de la relation contractuelle avec le collaborateur ou de son affectation à un service, étant entendu que les habilitations devront être supprimées immédiatement après la fin du contrat de travail ou dès le changement de service ;
- s'agissant des données de traçabilité : 1 an à compter de leur collecte.

Après en avoir délibéré, la Commission :

Constate que le présent traitement a également pour fonctionnalités :

- la collecte des évènements systèmes afin de tracer les accès des utilisateurs aux applications et aux données ;

- l'établissement de reportings.

Rappelle que :

- la liste nominative des personnes ayant accès au traitement, visée à l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993, doit être tenue à jour ;

- les Services de Police monégasques ne pourront avoir communication des informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées ;

- l'architecture technique repose sur des équipements de raccordements (switchs, routeurs, pare-feux) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés.

Fixe la durée de conservation des informations ainsi que suit :

- s'agissant de l'identité : 3 mois après le départ du collaborateur ;

- s'agissant des données d'identification électronique : la durée de la relation contractuelle avec le collaborateur ou de son affectation à un service, étant entendu que les habilitations devront être supprimées immédiatement après la fin du contrat de travail ou dès le changement de service ;

- s'agissant des données de traçabilité : 1 an à compter de leur collecte.

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 la succursale Crédit Agricole Monaco du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès avec traçabilité* ».**

Le Président

Guy MAGNAN